Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Windstream SIP Trunk Service with Avaya IP Office 10.1 and Avaya Session Border Controller for Enterprise 7.2 using UDP/RTP - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking between service provider Windstream and Avaya IP Office Release 10.1 and Avaya Session Border Controller for Enterprise Release 7.2 using UDP/RTP.

Windstream SIP Trunk Service provides PSTN access via a SIP trunk between the enterprise and the Windstream network as an alternative to legacy analog or digital trunks. This approach generally results in lower cost for the enterprise.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Windstream is a member of the Avaya DevConnect Service Provider program. Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

Table of Contents

1. Introduction

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking between Windstream and an Avaya IP Office solution. In the sample configuration, the Avaya IP Office solution consists of Avaya IP Office Release 10.1, Avaya embedded Voicemail, Avaya IP Office Application Server (with WebRTC and one-X Portal services enabled), Avaya Communicator for Windows (SIP mode), Avaya Communicator for Web, Avaya H.323, Avaya SIP, digital and analog deskphones. The enterprise solution connects to the Windstream network via the Avaya Session Border Controller for Enterprise (Avaya SBCE).

The Windstream referenced within these Application Notes is designed for business customers. The service enables local and long distance PSTN calling via standards-based SIP trunks as an alternative to legacy analog or digital trunks, without the need for additional TDM enterprise gateways and the associated maintenance costs.

.

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using Avaya IP Office connecting to Windstream via the Avaya SBCE.

This configuration (shown in **Figure 1**) was used to exercise the features and functionality tests listed in **Section 2.1**. **Note**: NAT devices added between Avaya SBCE and the Windstream network should be transparent to the SIP signaling.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member’s solution.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in this DevConnect Application Note included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

2.1. Interoperability Compliance Testing

A simulated enterprise site with Avaya IP Office and Avaya SBCE was connected to Windstream. To verify SIP trunking interoperability, the following features and functionality were exercised during the interoperability compliance test:

- Incoming PSTN calls to various phone types. Phone types included H.323, SIP, digital, and analog phones at the enterprise. All inbound PSTN calls were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various phone types. Phone types included H.323, SIP, digital, and analog phones at the enterprise. All outbound PSTN calls were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls from/to the Avaya Communicator for Windows (SIP)
- Inbound and outbound PSTN calls from/to the Avaya Communicator for Web with basic telephony transfer feature
- Inbound and outbound long hold time call stability
- Various call types including: local, long distance, international call, outbound toll-free, 411 local directory assistance, 911 emergency call
- SIP transport TLS/SRTP between Windstream and the simulated Avaya enterprise site
- Codec G.711MU and G.729A
- Caller number/ID presentation
- Privacy requests (i.e., caller anonymity) and Caller ID restriction for inbound and outbound calls
- DTMF transmission using RFC 2833
- Voicemail navigation for inbound and outbound calls
- Telephony features such as hold and resume, transfer, and conference
- Fax G.711 pass-through mode
- Off-net call forwarding
- Off-net call transfer: Use of SIP Re-Invite
- Twinning to mobile phones on inbound calls
- Remote Worker. Avaya Communicator for Windows (SIP) was used to test remote worker functionality

Item not supported include the following:

- Registration/Authentication
- TLS/SRTP SIP Transport
- Operator assisted call
- Inbound toll-free call
- Fax T.38
- Off-net call transfer: SIP Refer

2.2. Test Results

Interoperability testing of Windstream was completed with successful results for all test cases with the exception of the observation described below:

- SIP endpoints may indicate that a transfer failed even when it is successful: Occasionally on performing a transfer operation, Avaya IP Office SIP endpoints (Avaya 1100 Series Deskphone and Avaya Communicator for Windows) may indicate on the local call display that the transfer failed even though it was successful. The frequency of this behavior can be reduced by enabling “Emulate Notify for REFER” on the IP Office SIP Line (See **Section 5.6.2** - SIP advanced configuration).
- Windstream blocked those NPA and other international numbers from being forwarded due to fraud. Therefore, the off-net forward call was tested with only numbers setup in Windstream Lab during the compliance testing.
- Windstream did not support SIP Refer in off-net transfer call on the platform that Windstream used during the compliance testing. Instead, they preferred to use SIP Re-Invite.

2.3. Support

For technical support on the Avaya products described in these Application Notes visit: http://support.avaya.com.

For technical support on Windstream SIP Trunking, contact Windstream at https://www.windstreambusiness.com/solutions/voice-unified-communications/sip-trunking.
.

3. Reference Configuration

Figure 1 below illustrates the test configuration. The test configuration shows an enterprise site connected to Windstream through the public internet. For confidentiality and privacy purposes, actual public IP addresses and DID numbers used in this testing have been masked out and replaced with fictitious IP addresses throughout the document.

The Avaya components used to create the simulated customer site included:

- Avaya IP Office 500V2
- Avaya micro Session Border Controller for Enterprise
- Avaya embedded Voicemail for IP Office
- Avaya Application Server (Enabled WebRTC and one-X Portal services)
- Avaya 9600 Series IP Deskphones (H.323)
- Avaya 11x0 Series IP Deskphones (SIP)
- Avaya 1408 Digital phones
- Avaya Analog phones
- Avaya Communicator for Windows (SIP)
- Avaya Communicator for Web (WebRTC)
- Avaya Communicator for Windows (SIP) for remote worker

Located at the enterprise site are an Avaya Session Border Controller for Enterprise (Avaya SBCE), an Avaya IP Office 500V2 with the MOD DGTL STA16 expansion module which provides connections for 16 digital stations to the PSTN, and the extension PHONE 8 card which provides connections for 8 analog stations to the PSTN as well as 64-channel VCM (Voice Compression Module) for supporting VoIP codecs. The voicemail service is embedded on Avaya IP Office. Endpoints include Avaya 9600 Series IP Telephone (with H.323 firmware), Avaya 1100 Series IP Telephone (with SIP firmware), Avaya 1408D Digital Telephones, Avaya Analog Telephone, and Avaya Communicator for Windows.

The LAN2 port of Avaya IP Office was connected to the enterprise LAN while the LAN1 port was not used during the compliance test. The Avaya SBCE internal interface was connected to LAN2 port of the Avaya IP Office, while the Avaya SBCE external interface was connected to public internet.

A separate Windows 10 Enterprise PC runs Avaya IP Office Manager to configure and administer Avaya IP Office system.

Mobility Twinning is configured for some of the Avaya IP Office users so that calls to these user's phones will also ring and can be answered at configured mobile phones.

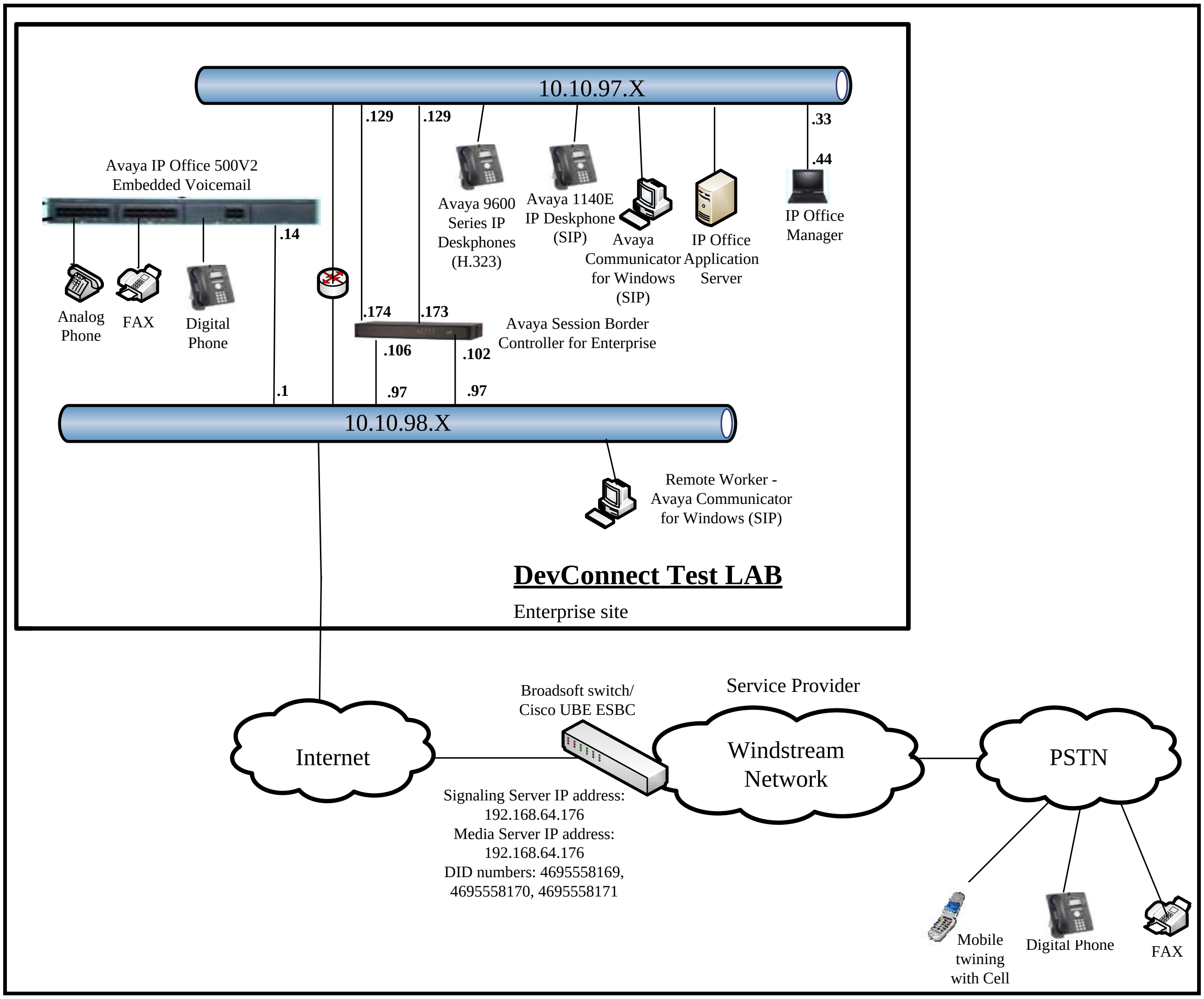


Figure 1 - Test Configuration for Avaya IP Office with Windstream SIP Trunk Service

For the purposes of the compliance test, Avaya IP Office users dialed a short code of 6 + N digits to send digits across the SIP trunk to Windstream. The short code of 6 was stripped off by Avaya IP Office but the remaining N digits were sent unaltered to Windstream. For calls within the North American Numbering Plan (NANP), the user would dial 11 (1 + 10) digits. Thus for these NANP calls, Avaya IP Office would send 11 digits in the Request URI and the To field of an outbound SIP INVITE message. It was configured to send 10 digits in the From field. For inbound calls, Windstream sent 10 digits in the Request URI and the To field of inbound SIP INVITE messages.

In an actual customer configuration, the enterprise site may also include additional network components between the service provider and Avaya SBCE, such as a data firewall. A complete discussion of the configuration of these devices is beyond the scope of these Application Notes.

However, it should be noted that SIP and RTP traffic between the service provider and Avaya SBCE must be allowed to pass through these devices.

4. Equipment and Software Validated

The following equipment and software/firmware were used for the sample configuration provided:

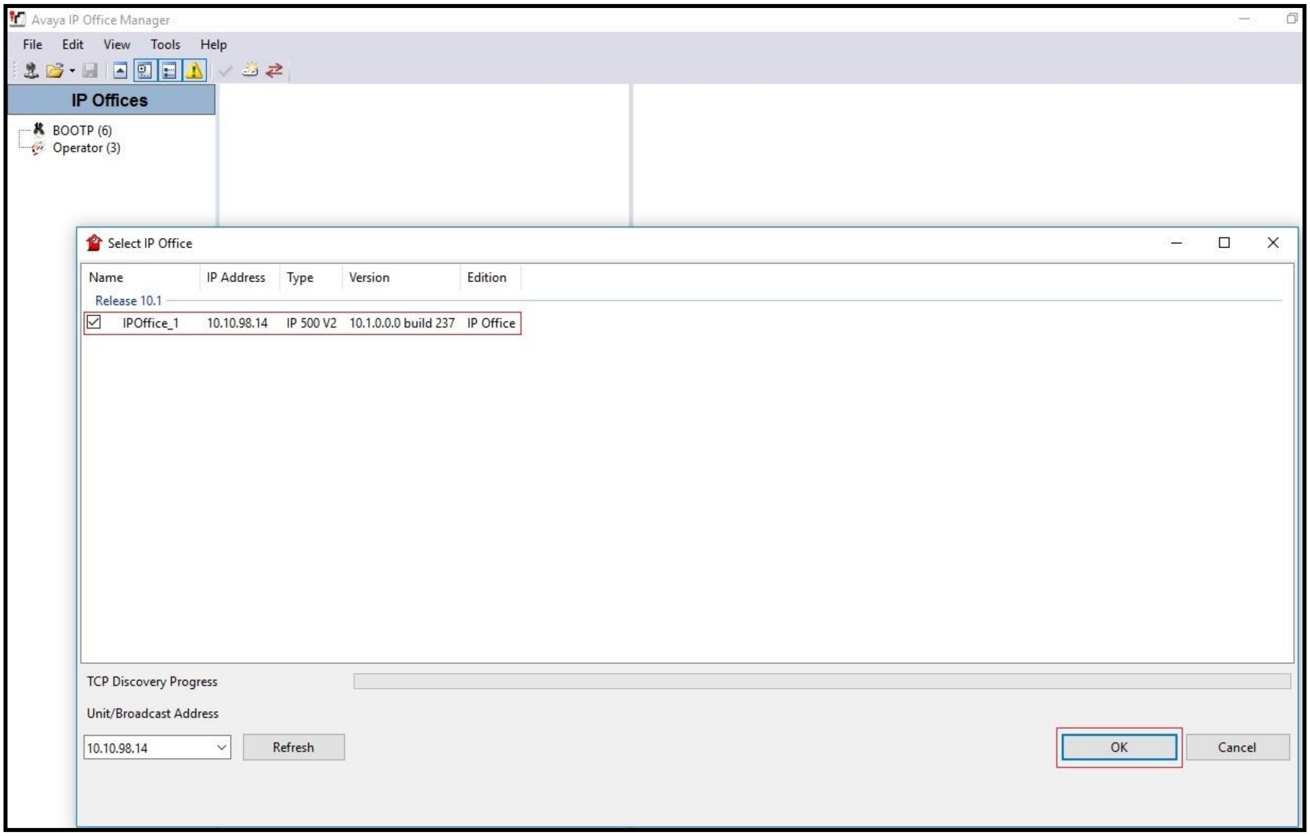
Avaya Telephony Components	
Equipment	**Release**
Avaya IP Office solution • Avaya IP Office 500V2 • Embedded Voicemail • Avaya Web RTC Gateway • Avaya one-X Portal • Avaya IP Office Manager • Avaya IP Office Analogue PHONE 8 • Avaya IP Office VCM64/PRID U • Avaya IP Office DIG DCPx16 V2	10.1.0.0.0 build 237 10.1.0.0.0 build 237 10.1.0.0.0 build 13 10.1.0.0.0 build 305 10.1.0.0.0 build 237 10.1.0.0.0 build 237 10.1.0.0.0 build 237 10.1.0.0.0 build 237
Avaya Session Border Controller for Enterprise	7.2.0.0-18-13712
Avaya 1140E IP Deskphone (SIP)	04.04.23
Avaya 9641G IP Deskphone (H.323)	6.6.4.01
Avaya 9621G IP Deskphone (H.323)	6.6.4.01
Avaya Communicator for Windows (SIP)	2.1.4.0 - 256
Avaya Communicator for Web	1.0.16.1718
Avaya 1408D Digital Deskphone	R46
Avaya Analog Deskphone	N/A
HP Officejet 4500 (fax)	N/A
Windstream Components	
Equipment	**Release**
Broadsoft switch	R20 SP1
Cisco UBE ESBC	c2900-universalk9-mz.SPA.154-3.M5

Note: Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office 500V2 and also when deployed with IP Office in all configurations.

5. Configure Avaya IP Office Solution

This section describes the Avaya IP Office solution configuration necessary to support connectivity to the Avaya SBCE. It is assumed that the initial installation and provisioning of the Avaya IP Office 500V2 has been previously completed and therefore is not covered in these Application Notes. For information on these installation tasks refer to Additional References **Section 10**.

This section describes the Avaya IP Office configuration required to support connectivity to the Avaya SBCE. Avaya IP Office is configured through the Avaya IP Office Manager PC application. From a PC running the Avaya IP Office Manager application, select **Start → Programs → IP Office → Manager** to launch the application. Navigate to **File → Open Configuration**, select the proper Avaya IP Office system from the pop-up window and click **OK** button. Log in using appropriate credentials.



Name	IP Address	Type	Version	Edition
Release 10.1				
☑ IPOffice_1	10.10.98.14	IP 500 V2	10.1.0.0.0 build 237	IP Office

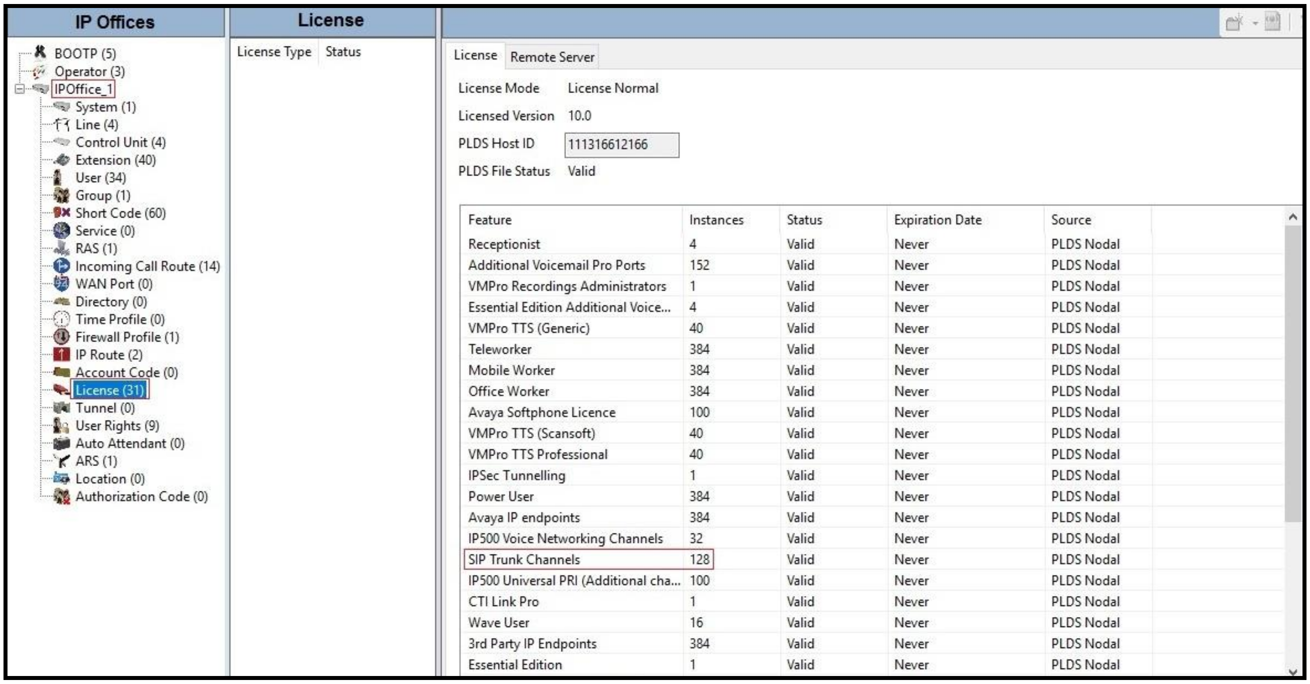
Unit/Broadcast Address: 10.10.98.14

Figure 2 – Avaya IP Office Selection

5.1. Licensing

The configuration and features described in these Application Notes require the Avaya IP Office system to be licensed appropriately. If a desired feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative.

To verify that there is a SIP Trunk Channels license with sufficient capacity, select **IPOffice_1 → License** on the Navigation pane and **SIP Trunk Channels** in the Group pane. Confirm that there is a valid license with sufficient "Instances" (trunk channels) in the **Details** pane.



License Mode License Normal

Licensed Version 10.0

PLDS Host ID 111316612166

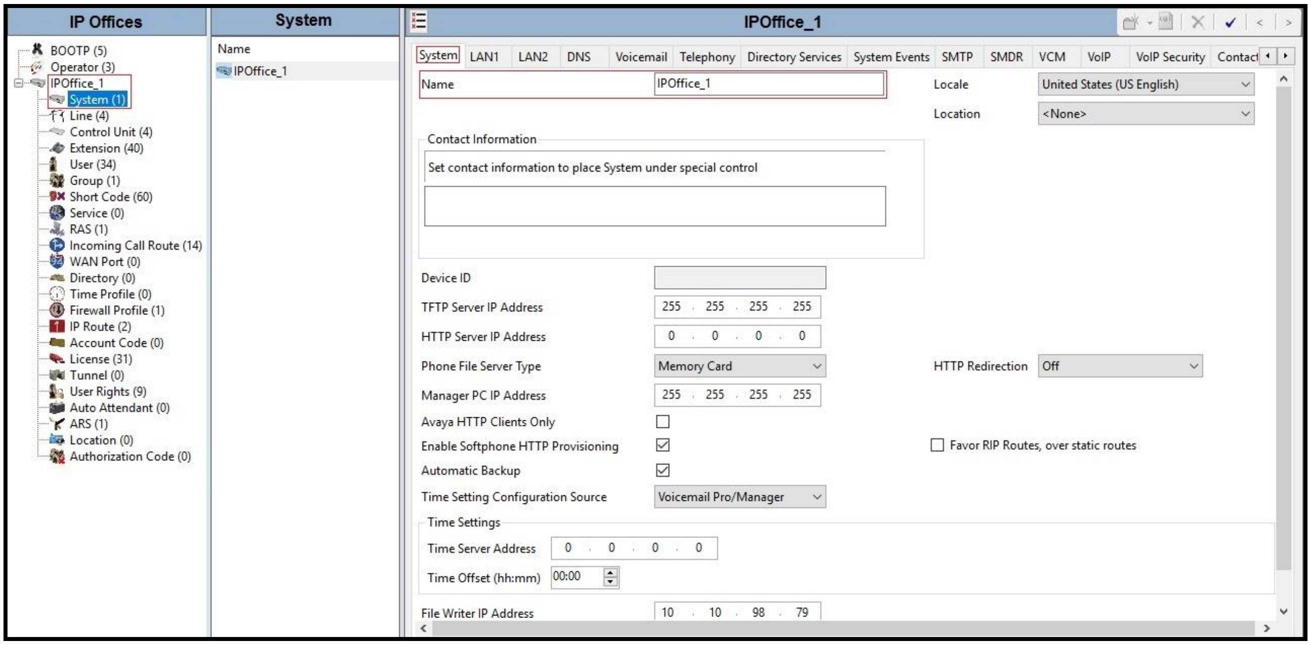
PLDS File Status Valid

Feature	Instances	Status	Expiration Date	Source
Receptionist	4	Valid	Never	PLDS Nodal
Additional Voicemail Pro Ports	152	Valid	Never	PLDS Nodal
VMPro Recordings Administrators	1	Valid	Never	PLDS Nodal
Essential Edition Additional Voice...	4	Valid	Never	PLDS Nodal
VMPro TTS (Generic)	40	Valid	Never	PLDS Nodal
Teleworker	384	Valid	Never	PLDS Nodal
Mobile Worker	384	Valid	Never	PLDS Nodal
Office Worker	384	Valid	Never	PLDS Nodal
Avaya Softphone Licence	100	Valid	Never	PLDS Nodal
VMPro TTS (Scansoft)	40	Valid	Never	PLDS Nodal
VMPro TTS Professional	40	Valid	Never	PLDS Nodal
IPSec Tunnelling	1	Valid	Never	PLDS Nodal
Power User	384	Valid	Never	PLDS Nodal
Avaya IP endpoints	384	Valid	Never	PLDS Nodal
IP500 Voice Networking Channels	32	Valid	Never	PLDS Nodal
SIP Trunk Channels	128	Valid	Never	PLDS Nodal
IP500 Universal PRI (Additional cha...	100	Valid	Never	PLDS Nodal
CTI Link Pro	1	Valid	Never	PLDS Nodal
Wave User	16	Valid	Never	PLDS Nodal
3rd Party IP Endpoints	384	Valid	Never	PLDS Nodal
Essential Edition	1	Valid	Never	PLDS Nodal

Figure 3 – Avaya IP Office License

5.2. System Tab

Navigate to **System (1)** under **IPOffice_1** on the left pane and select the **System** tab in the **Details** pane. The **Name** field can be used to enter a descriptive name for the system. In the reference configuration, **IPOffice_1** was used as the name in IP Office.



Name: IPOffice_1
Locale: United States (US English)
Location: <None>

Contact Information
Set contact information to place System under special control

Device ID:
TFTP Server IP Address: 255 . 255 . 255 . 255
HTTP Server IP Address: 0 . 0 . 0 . 0
Phone File Server Type: Memory Card
HTTP Redirection: Off
Manager PC IP Address: 255 . 255 . 255 . 255
Avaya HTTP Clients Only: □
Enable Softphone HTTP Provisioning: ☑
□ Favor RIP Routes, over static routes
Automatic Backup: ☑
Time Setting Configuration Source: Voicemail Pro/Manager

Time Settings
Time Server Address: 0 . 0 . 0 . 0
Time Offset (hh:mm): 00:00

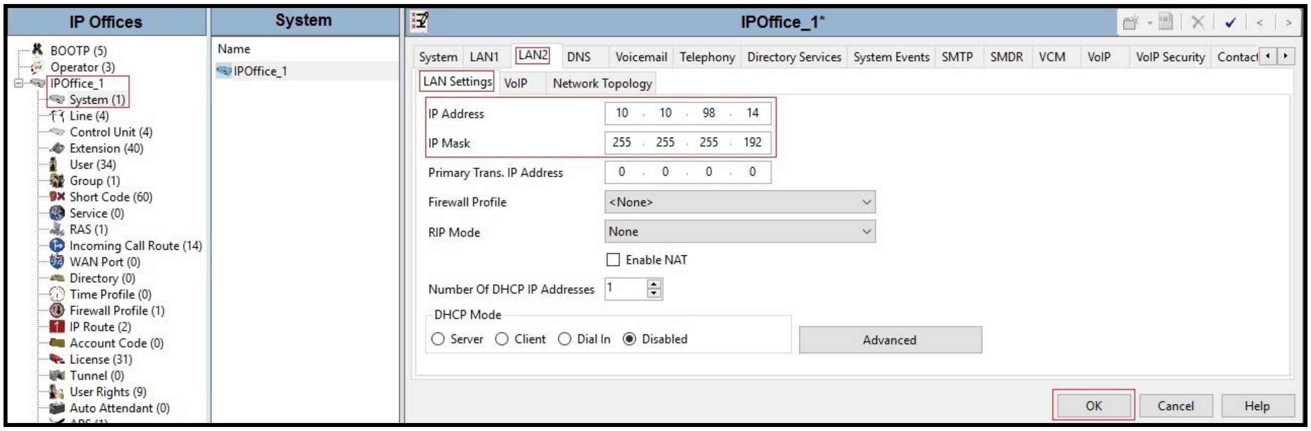
File Writer IP Address: 10 . 10 . 98 . 79

Figure 4 - Avaya IP Office System Configuration

5.3. LAN2 Settings

In the sample configuration, LAN2 is used to connect the enterprise network to Avaya SBCE.

To configure the LAN2 settings on the IP Office, complete the following steps. Navigate to **IPOffice_1 → System (1)** in the **Navigation** and **Group** panes and then navigate to the **LAN2 → LAN Settings** tab in the **Details** pane. Set the **IP Address** field to the IP address assigned to the Avaya IP Office LAN2 port. Set the **IP Mask** field to the mask used on the private network. All other parameters should be set according to customer requirements. Click **OK** to submit the change.



IP Address: 10 . 10 . 98 . 14

IP Mask: 255 . 255 . 255 . 192

Primary Trans. IP Address: 0 . 0 . 0 . 0

Firewall Profile: <None>

RIP Mode: None

☐ Enable NAT

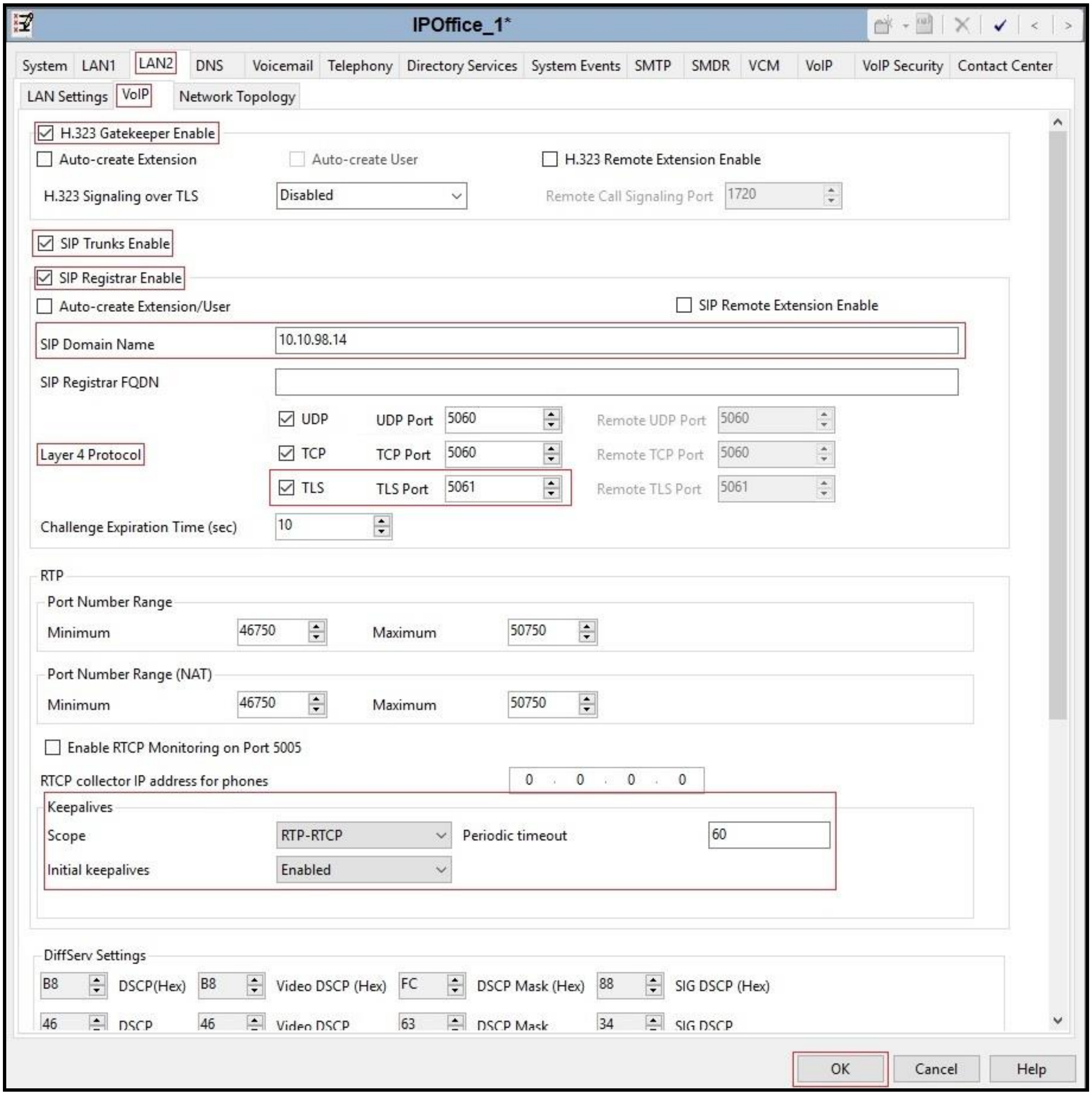
Number Of DHCP IP Addresses: 1

DHCP Mode: ○ Server ○ Client ○ Dial In ● Disabled

Figure 5 - Avaya IP Office LAN2 Settings

The **VoIP** tab as shown in the screenshot below was configured with following settings:

- Check the **H323 Gatekeeper Enable** to allow Avaya IP deskphones/softphones using the H.323 protocol to register
- Check the **SIP Trunks Enable** to enable the configuration of SIP Trunk connecting to Windstream via Avaya SBCE
- Check the **SIP Registrar Enable** to allow Avaya IP deskphones/softphones to register using the SIP protocol
- Input **SIP Domain Name** as **10.10.98.14**
- The **Layer 4 Protocol** uses **TLS** with **TLS Port** as **5061**
- Verify **Keepalives** to select **Scope** as **RTP-RTCP** with **Periodic timeout 60** and select **Initial keepalives** as **Enabled**
- All other parameters should be set according to customer requirements
- Click **OK** to submit the changes


IPOffice_1*
System | LAN1 | LAN2 | DNS | Voicemail | Telephony | Directory Services | System Events | SMTP | SMDR | VCM | VoIP | VoIP Security | Contact Center
LAN Settings | VoIP | Network Topology
OK | Cancel | Help

☑ H.323 Gatekeeper Enable

☐ Auto-create Extension ☐ Auto-create User ☐ H.323 Remote Extension Enable

H.323 Signaling over TLS: Disabled

Remote Call Signaling Port: 1720

☑ SIP Trunks Enable

☑ SIP Registrar Enable

☐ Auto-create Extension/User ☐ SIP Remote Extension Enable

SIP Domain Name: 10.10.98.14

SIP Registrar FQDN:

Layer 4 Protocol:

☑ UDP	UDP Port	5060	Remote UDP Port	5060
☑ TCP	TCP Port	5060	Remote TCP Port	5060
☑ TLS	TLS Port	5061	Remote TLS Port	5061

Challenge Expiration Time (sec): 10

RTP

Port Number Range: Minimum 46750 Maximum 50750

Port Number Range (NAT): Minimum 46750 Maximum 50750

☐ Enable RTCP Monitoring on Port 5005

RTCP collector IP address for phones: 0 . 0 . 0 . 0

Keepalives

Scope: RTP-RTCP Periodic timeout: 60

Initial keepalives: Enabled

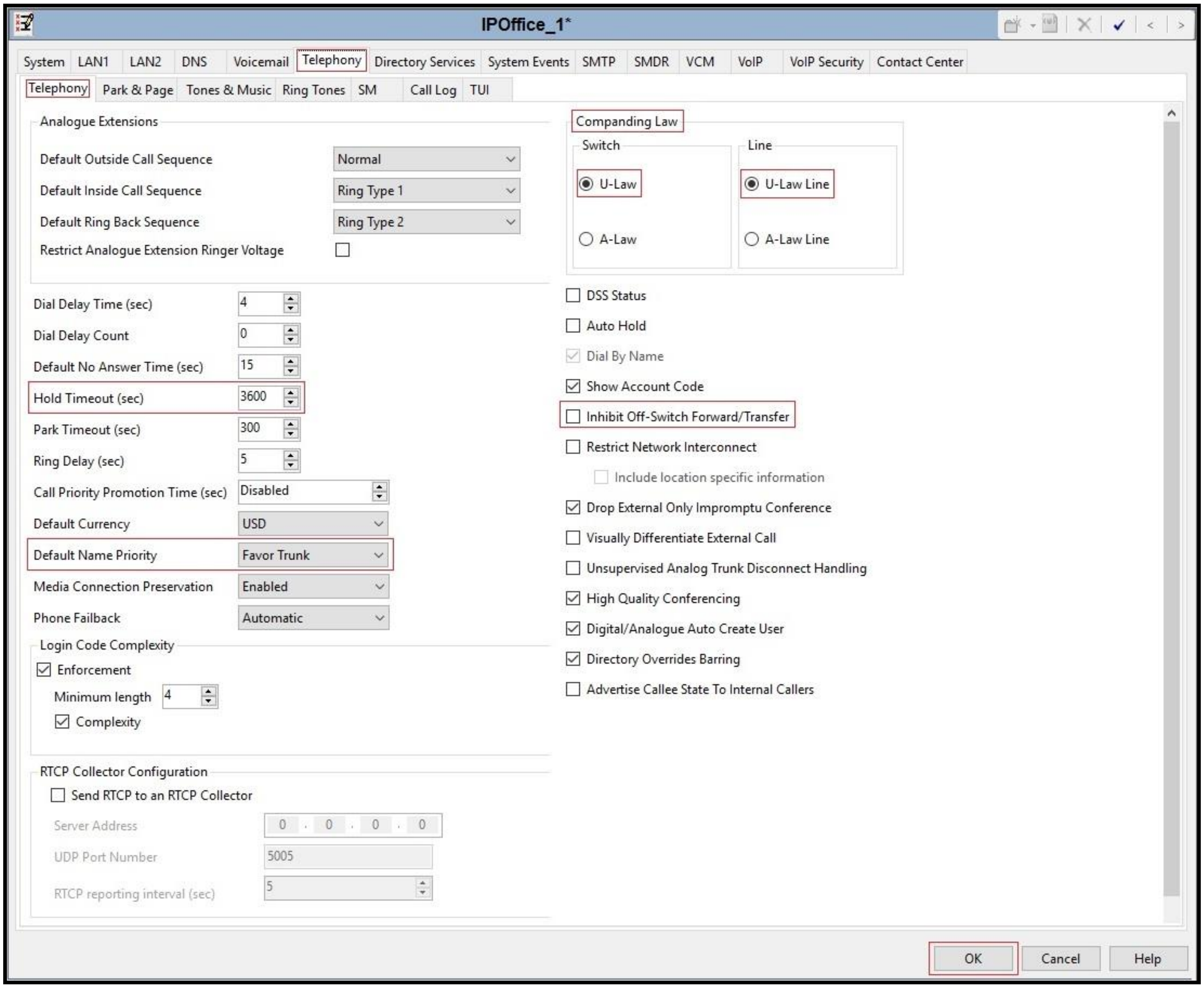
DiffServ Settings

B8	DSCP(Hex)	B8	Video DSCP (Hex)	FC	DSCP Mask (Hex)	88	SIG DSCP (Hex)
46	DSCP	46	Video DSCP	63	DSCP Mask	34	SIG DSCP

Figure 6 - Avaya IP Office LAN2 VoIP

5.4. System Telephony Settings

Navigate to **IPOffice_1 → System (1)** in the Navigation and Group Panes (not shown) and then navigate to the **Telephony → Telephony** tab in the **Details** pane. Choose the **Companding Law** typical for the enterprise location. For North America, **U-Law** is used. Uncheck the **Inhibit Off-Switch Forward/Transfer** box to allow call forwarding and call transfers to the PSTN via the service provider across the SIP trunk. Set **Hold Timeout (sec)** to a valid number. Set **Default Name Priority** to **Favor Trunk**. Defaults were used for all other settings. Click **OK** to submit the changes.



Analogue Extensions

Default Outside Call Sequence: Normal

Default Inside Call Sequence: Ring Type 1

Default Ring Back Sequence: Ring Type 2

Restrict Analogue Extension Ringer Voltage □

Dial Delay Time (sec): 4

Dial Delay Count: 0

Default No Answer Time (sec): 15

Hold Timeout (sec): 3600

Park Timeout (sec): 300

Ring Delay (sec): 5

Call Priority Promotion Time (sec): Disabled

Default Currency: USD

Default Name Priority: Favor Trunk

Media Connection Preservation: Enabled

Phone Failback: Automatic

Login Code Complexity

☑ Enforcement

Minimum length: 4

☑ Complexity

RTCP Collector Configuration

□ Send RTCP to an RTCP Collector

Server Address: 0 . 0 . 0 . 0

UDP Port Number: 5005

RTCP reporting interval (sec): 5

Companding Law

Switch: ● U-Law ○ A-Law

Line: ● U-Law Line ○ A-Law Line

□ DSS Status

□ Auto Hold

☑ Dial By Name

☑ Show Account Code

□ Inhibit Off-Switch Forward/Transfer

□ Restrict Network Interconnect

□ Include location specific information

☑ Drop External Only Impromptu Conference

□ Visually Differentiate External Call

□ Unsupervised Analog Trunk Disconnect Handling

☑ High Quality Conferencing

☑ Digital/Analogue Auto Create User

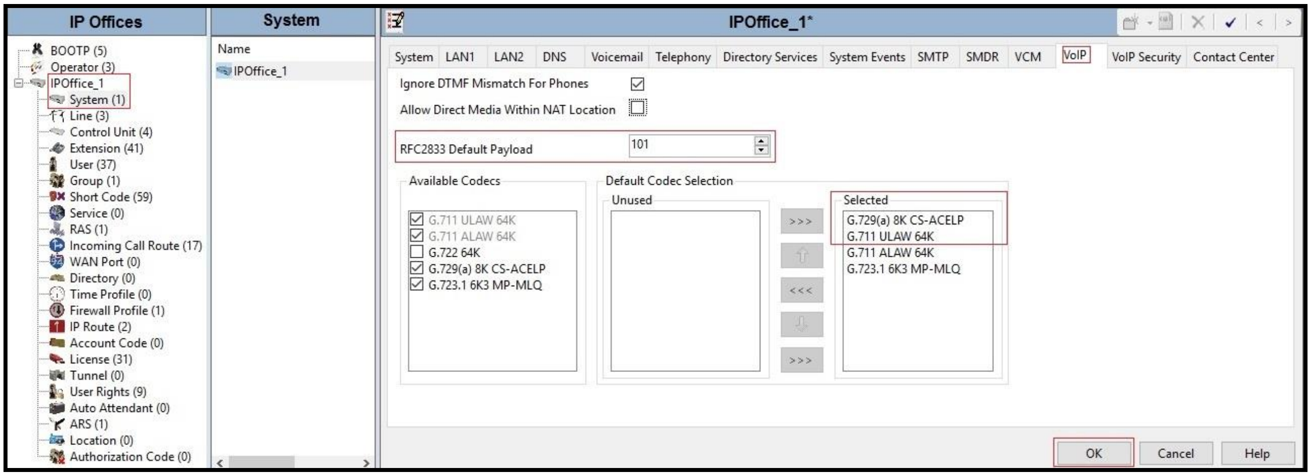
☑ Directory Overrides Barring

□ Advertise Callee State To Internal Callers

Figure 7 - Avaya IP Office Telephony

5.5. System VoIP Settings

Navigate to **IPOffice_1 → System (1)** in the Navigation and Group Panes and then navigate to the **VoIP** tab in the **Details** pane. Leave the **RFC2833 Default Payload** as default of **101**. Select codec **G.729(a) 8K CS-ACEL**P, **G.711 ULAW 64K** which Windstream supports. Click **OK** to submit the changes.



Ignore DTMF Mismatch For Phones ☑

Allow Direct Media Within NAT Location ☐

RFC2833 Default Payload: 101

Available Codecs

- ☑ G.711 ULAW 64K
- ☑ G.711 ALAW 64K
- ☐ G.722 64K
- ☑ G.729(a) 8K CS-ACELP
- ☑ G.723.1 6K3 MP-MLQ

Default Codec Selection

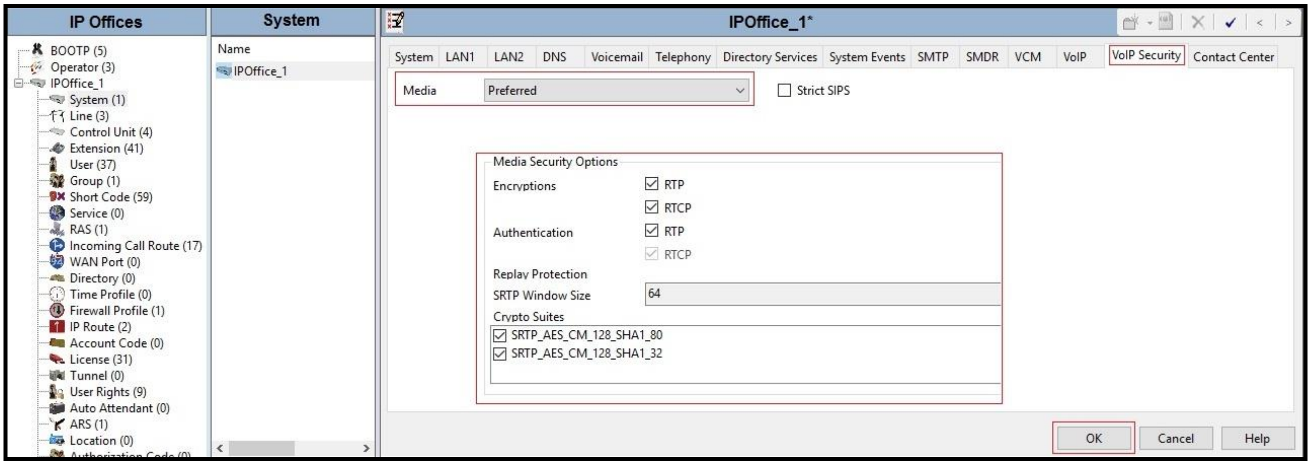
Unused

Selected

- G.729(a) 8K CS-ACELP
- G.711 ULAW 64K
- G.711 ALAW 64K
- G.723.1 6K3 MP-MLQ

Figure 8 - Avaya IP Office VoIP

Navigate to **IPOffice_1 → System (1)** in the Navigation and Group Panes and then navigate to the **VoIP Security** tab in the **Details** pane. Select **Media** as **Preferred** and select **Media Security Options** as highlights. Click **OK** to submit the changes.



Media: Preferred

☐ Strict SIPS

Media Security Options

Encryptions ☑ RTP ☑ RTCP

Authentication ☑ RTP ☑ RTCP

Replay Protection

SRTP Window Size: 64

Crypto Suites

- ☑ SRTP_AES_CM_128_SHA1_80
- ☑ SRTP_AES_CM_128_SHA1_32

Figure 9 - Avaya IP Office VoIP Security

5.6. Administer SIP Line

A SIP Line is needed to establish the SIP connection between Avaya IP Office and Avaya SBCE. The recommended method for configuring a SIP Line is to use the template associated with these Application Notes. The template is an .xml file that can be used by Avaya IP Office Manager to create a SIP Line. Follow the steps in **Section 5.6.1** to create the SIP Line from the template.

Some items relevant to a specific customer environment are not included in the template or may need to be updated after the SIP Line is created. Examples include the following:

- IP addresses
- SIP Credentials (if applicable)
- SIP URI entries
- Setting of the Use Network Topology Info field on the Transport tab.

Therefore, it is important that the SIP Line configuration be reviewed and updated if necessary after the SIP Line is created via the template. The resulting SIP Line data can be verified against the manual configuration shown in **Section 5.6.2**.

Also, the following SIP Line settings are not supported on Basic Edition:

- SIP Line – Originator number for forwarded and twinning calls
- Transport – Second Explicit DNS Server
- SIP Credentials – Registration Required
- SIP Advanced Engineering

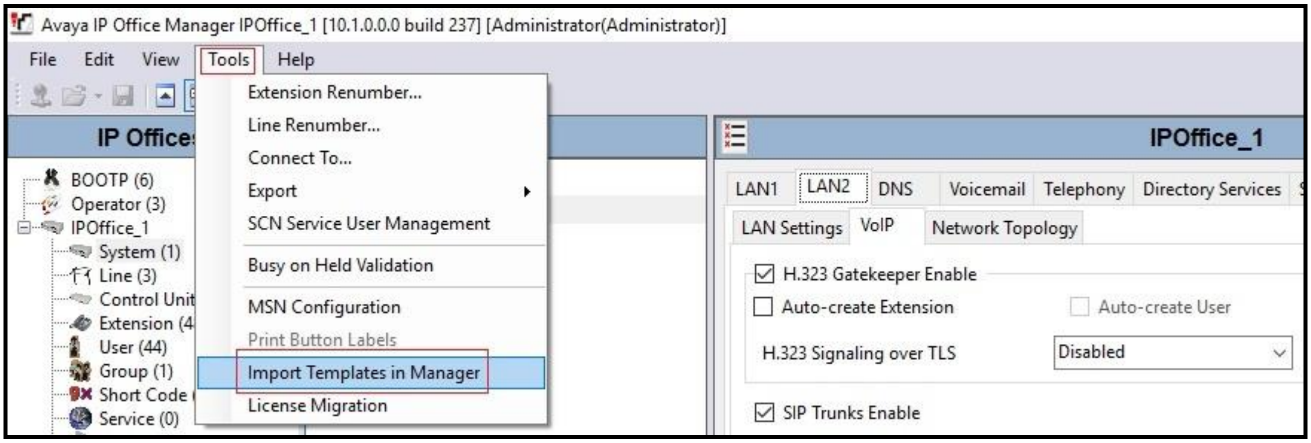
Alternatively, a SIP Line can be created manually. To do so, right-click **Line** in the Navigation Pane and select **New → SIP Line**. Then, follow the steps outlined in **Section 5.6.2**.

For the compliance test, SIP Line 17 was used as trunk for both outgoing and incoming calls.

5.6.1. Create SIP Line from Template

This section describes the steps to create a SIP line from the template as follows:

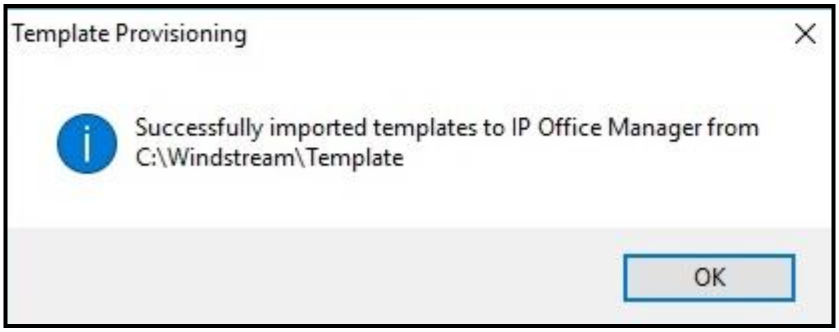
1. Create a new folder in computer where Avaya IP Office Manager is installed (e.g. C:\Windstream\Template). Copy the template file to this folder. The template file for the compliance test is **WSIPO101SBC72.xml** (for SIP Line 17).
2. Import the template into Avaya IP Office Manager: From Avaya IP Office Manager, select **Tools → Import Templates in Manager**. This action will copy the template file from step 1 into the IP Office template directory.



☑ H.323 Gatekeeper Enable
☐ Auto-create Extension ☐ Auto-create User
H.323 Signaling over TLS: Disabled
☑ SIP Trunks Enable

Figure 10 – Import Template for SIP Line

In the pop-up window (not shown) that appears, select the folder where the template file was copied in step 1. After the import is complete, a final import status pop-up window below will appear stating success (or failure). Then click **OK** to continue.


Template Provisioning

Successfully imported templates to IP Office Manager from C:\Windstream\Template

Figure 11 – Import Template for SIP Line successfully

3. Create the SIP Trunk from the template: Right-click on **Line** in the Navigation Pane, then navigate to **New from Template → Open from file**.

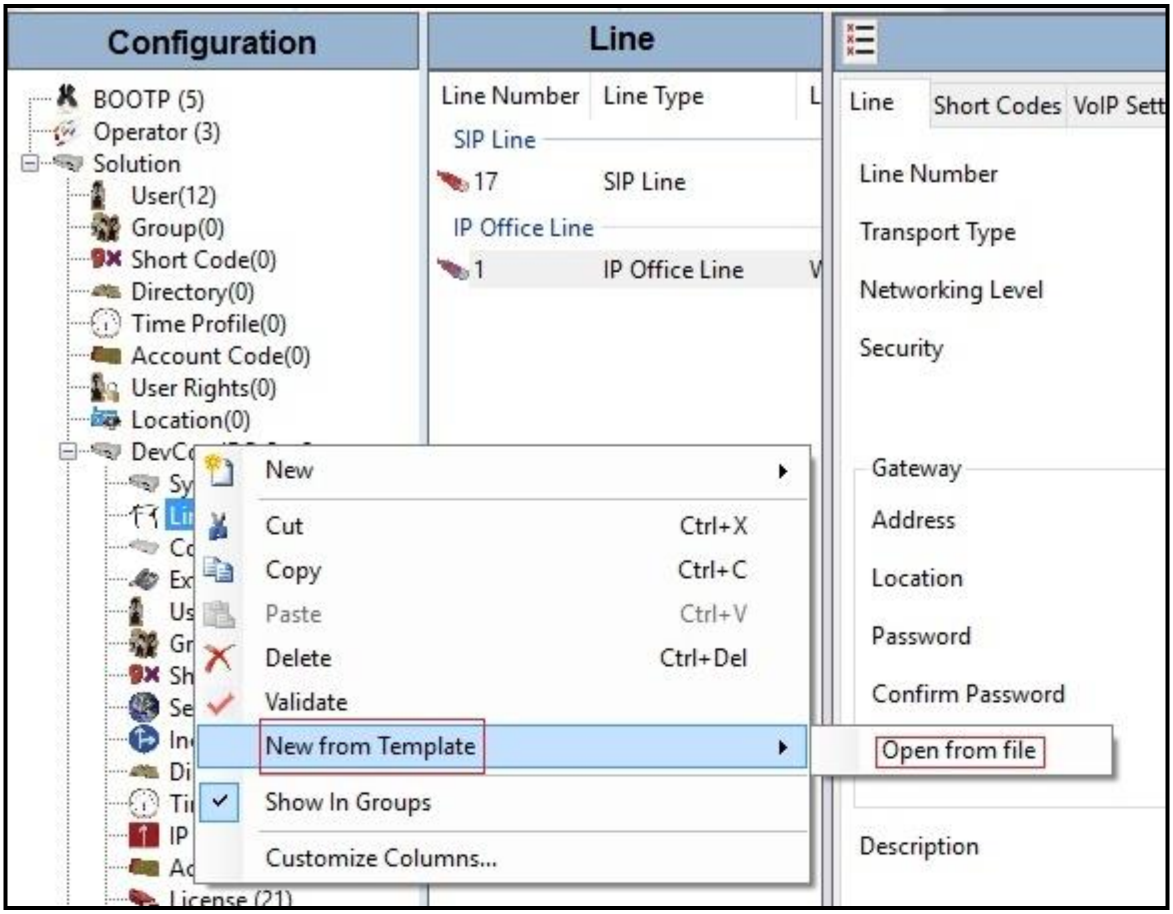
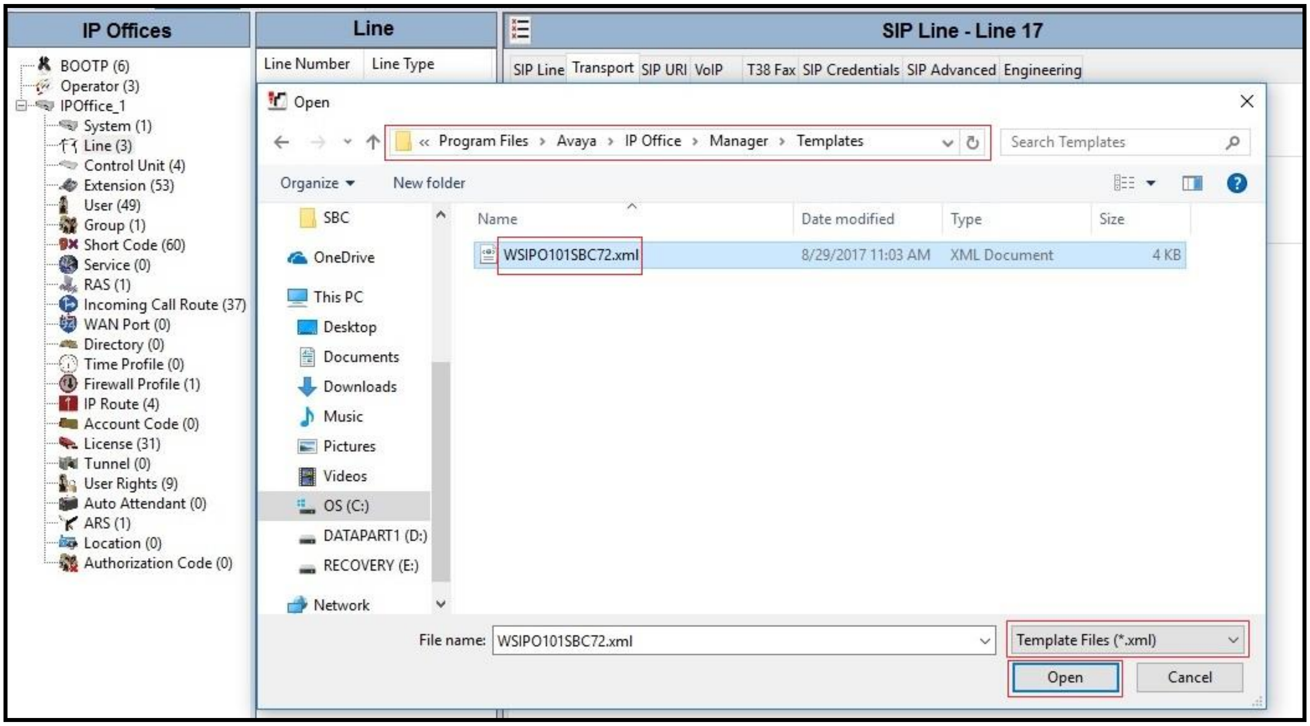


Figure 12 – Create SIP Line from Template

4. Select the **Template Files (*.xml)** and select the imported template from step 2 at IP Office template directory **C:\Program Files\Avaya\IP Office\Manager\Templates\**. Click **Open** button to create a SIP line from template.



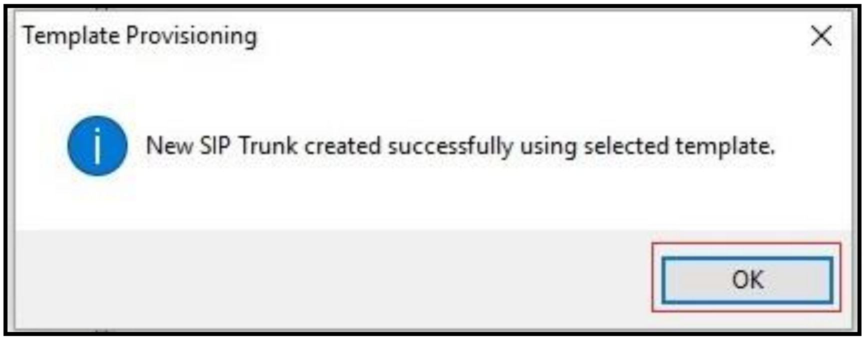
Name	Date modified	Type	Size
WSIPO101SBC72.xml	8/29/2017 11:03 AM	XML Document	4 KB

File name: WSIPO101SBC72.xml

Template Files (*.xml)

Figure 13 – Create SIP Line from IP Office Template directory

A pop-up window below will appear stating success (or failure). Then click **OK** to continue.



Template Provisioning

New SIP Trunk created successfully using selected template.

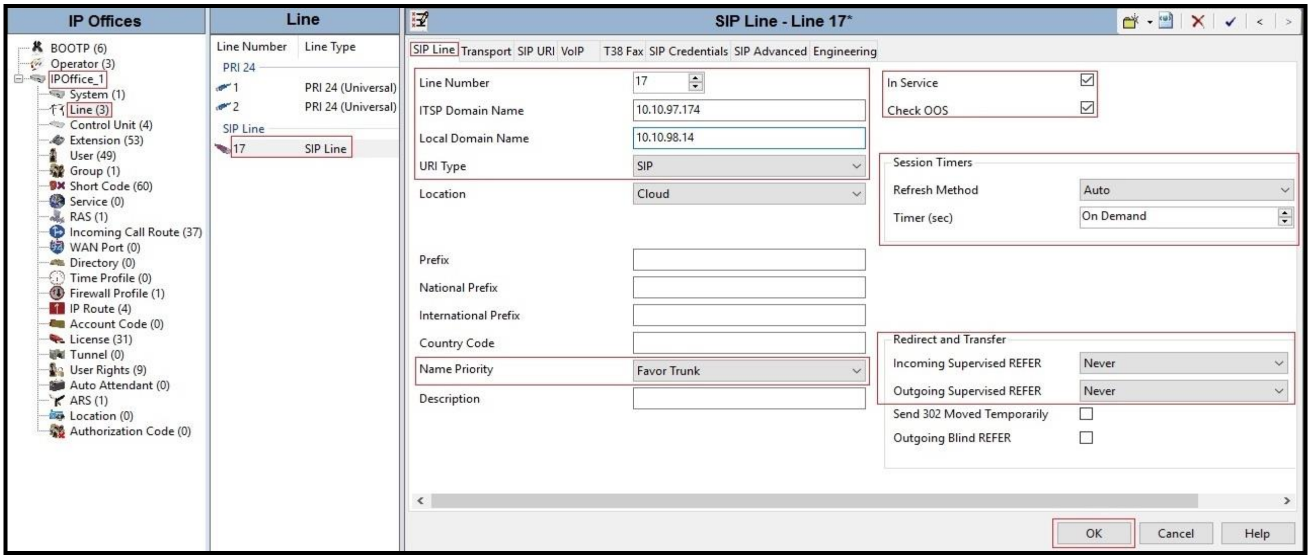
Figure 14 – Create SIP Line from Template successfully

5. Once the SIP Line is created, verify the configuration of the SIP Lines with the configuration shown in **Section 5.6.2**.

5.6.2. Create SIP Line Manually

To create a SIP line, begin by navigating to **Line** in the left Navigation Pane, then right-click in the Group Pane and select **New → SIP Line** (not shown).
On the **SIP Line** tab in the Details Pane, configure the parameters as shown below:

- Select available **Line Number**: **17**
- Set **ITSP Domain Name** to the IP address of Avaya SBCE internal interface. This field is used to specify the default host part of the SIP URI in the To, R-URI fields for outgoing calls
- Set **Local Domain Name** to IP address of Avaya IP Office LAN2 port. This field is used to specify the default host part of the SIP URI in the From field for outgoing calls
  Note: For the user making the call, the user part of the From SIP URI is determined by the settings of the SIP URI channel record being used to route the call (see SIP URI → Local URI). For the destination of the call, the user part of the To and R-URI fields are determined by dial short codes of the form 6N;/N where N is the user part of the SIP URI
- Check the **In Service** and **Check OOS** boxes
- Set **URI Type** to **SIP**
- For **Session Timers**, set **Refresh Method** to **Auto** with **Timer (sec)** to **On Demand**
- Set **Name Priority** to **Favor Trunk**. As described in **Section 5.4**, the **Default Name Priority** parameter may retain the default **Favor Trunk** setting, or can be configured to **Favor Directory**. As shown below, the default **Favor Trunk** setting was used in the reference configuration
- For **Redirect and Transfer**, set **Incoming Supervised REFER** and **Outgoing Supervised REFER** to **Never**. Note: Windstream does not support SIP REFER for off-net transfer call during the compliance testing
- Default values may be used for all other parameters
- Click **OK** to commit then press Ctrl + S to save



Line

Line Number	Line Type
PRI 24	
1	PRI 24 (Universal)
2	PRI 24 (Universal)
SIP Line	
17	SIP Line

Line Number	17
ITSP Domain Name	10.10.97.174
Local Domain Name	10.10.98.14
URI Type	SIP
Location	Cloud
Prefix	
National Prefix	
International Prefix	
Country Code	
Name Priority	Favor Trunk
Description	
In Service	☑
Check OOS	☑

Session Timers

Refresh Method	Auto
Timer (sec)	On Demand

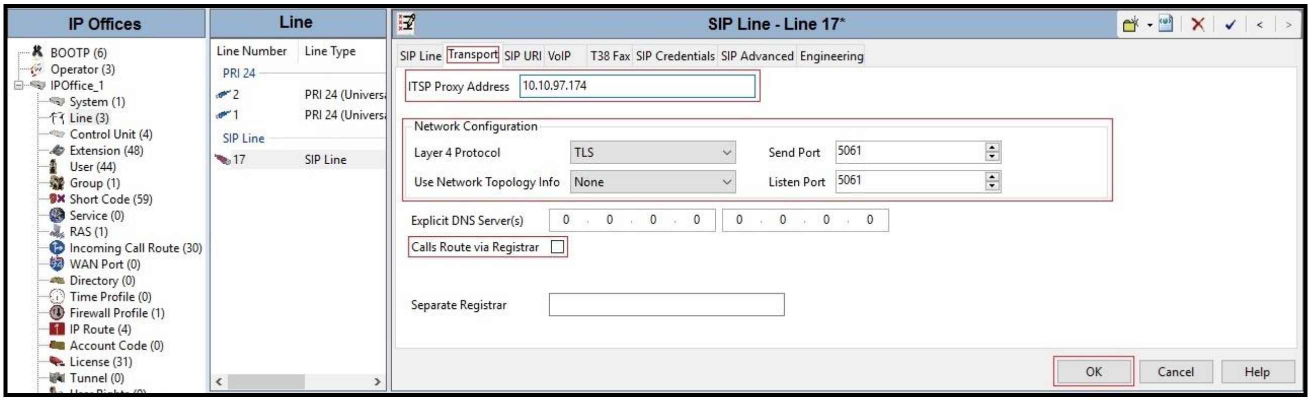
Redirect and Transfer

Incoming Supervised REFER	Never
Outgoing Supervised REFER	Never
Send 302 Moved Temporarily	☐
Outgoing Blind REFER	☐

Figure 15 – SIP Line Configuration

On the **Transport** tab in the Details Pane, configure the parameters as shown below:

- The **ITSP Proxy Address** was set to the IP address of Avaya SBCE internal interface: **10.10.97.174** as shown in **Figure 1**
- In the **Network Configuration** area, **TLS** was selected as the **Layer 4 Protocol** and the **Send Por**t was set to **5061**
- The **Use Network Topology Info** parameter was set to **None**. The **Listen Port** was set to **5061**. Note: For the compliance testing, the **Use Network Topology Info** field was set to **None**, since no NAT was using in the test configuration. In addition, it was not necessary to configure the **System → LAN2 → Network Topology** tab for the purposes of SIP trunking. If a NAT is used between Avaya IP Office and the other end of the trunk, then the **Use Network Topology Info** field should be set to the LAN interface (**LAN2**) used by the trunk and the **System → LAN2 → Network Topology** tab needs to be configured with the details of the NAT device
- The **Calls Route via Registrar** was unchecked. In this certification testing, Windstream did not support the dynamic Registration on the SIP Trunk
- Other parameters retain default values
- Click **OK** to commit then press Ctrl + S to save



ITSP Proxy Address: 10.10.97.174

Layer 4 Protocol: TLS
Send Port: 5061
Use Network Topology Info: None
Listen Port: 5061

Explicit DNS Server(s): 0 . 0 . 0 . 0 0 . 0 . 0 . 0

Calls Route via Registrar ☐

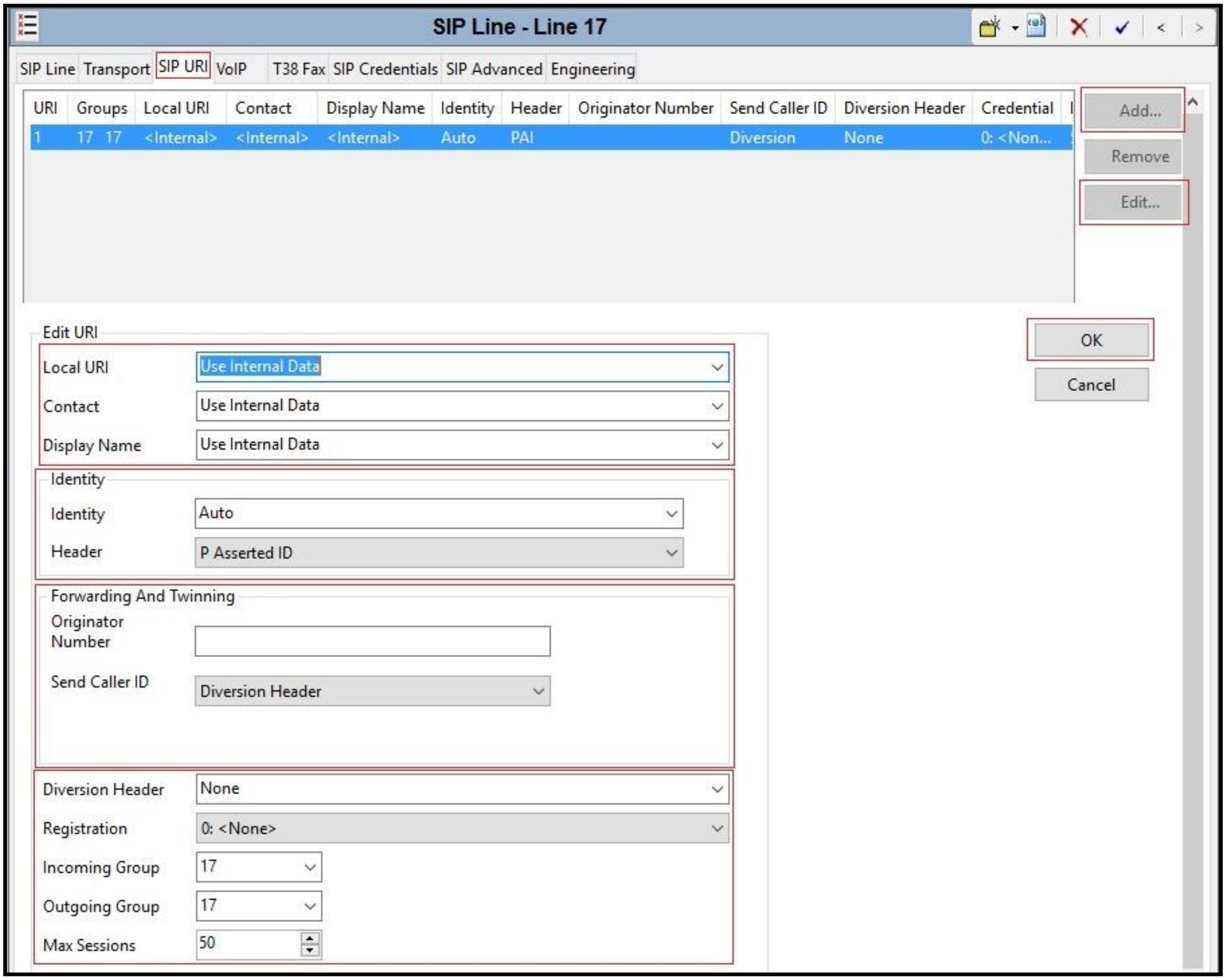
Separate Registrar:

Figure 16 – SIP Line Transport Configuration

The SIP URI entry must be created to match any DID number assigned to an Avaya IP Office user and Avaya IP Office will route the calls on this SIP line. Select the **SIP URI** tab; click the **Add** button and the **New Channel** area will appear at the bottom of the pane (not shown). To edit an existing entry, click an entry in the list at the top, and click **Edit…** button. In the example screen below, a previously configured entry is edited.

A SIP URI entry was created that matched any DID number assigned to an Avaya IP Office user. The entry was created with the parameters shown below:

- Set **Local URI**, **Contact**, and **Display Name** to **Use Internal Data**. This setting allows calls on this line whose SIP URI matches the number set in the **SIP** tab of any **User** as shown in **Section 5.8**
- For **Identity**, set **Identity** to **Auto** and **Header** to **P Asserted ID**
- For **Forwarding And Twinning**, set **Send Caller ID** to **Diversion Header**
  Note: When using the twinning feature, the calling party number displayed on the twinned phone is controlled by the **Send Caller ID** parameter
- Leave **Diversion Header** to **None** by default
- Set **Registration** to **0: <None>**
- Associate this line with an incoming line group in the **Incoming Group** field and an outgoing line group in the **Outgoing Group** field. This line group number will be used in defining incoming and outgoing call routes for this line. For the compliance test, a new line group **17** was defined that only contains this line (line 17)
- Set **Max Sessions** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern
- Click **OK** to submit the changes



URI	Groups	Local URI	Contact	Display Name	Identity	Header	Originator Number	Send Caller ID	Diversion Header	Credential	I
1	17 17	<Internal>	<Internal>	<Internal>	Auto	PAI		Diversion	None	0: <Non...	

Edit URI

Local URI: Use Internal Data

Contact: Use Internal Data

Display Name: Use Internal Data

Identity

Identity: Auto

Header: P Asserted ID

Forwarding And Twinning

Originator Number:

Send Caller ID: Diversion Header

Diversion Header: None

Registration: 0: <None>

Incoming Group: 17

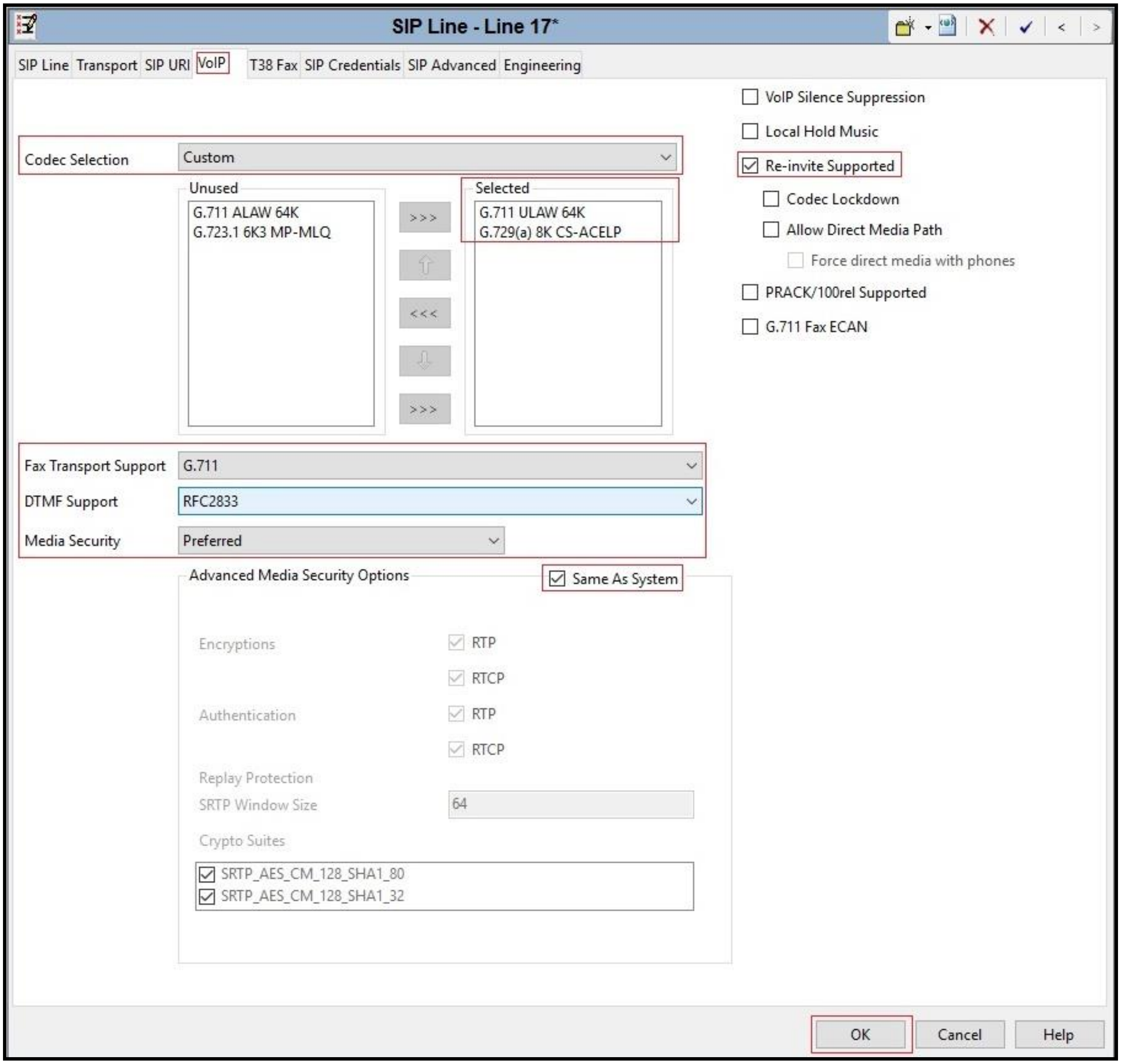
Outgoing Group: 17

Max Sessions: 50

Figure 17 – SIP Line SIP URI Configuration

Select the **VoIP** tab to set the Voice over Internet Protocol parameters of the SIP line. Set the parameters as shown below:

- The **Codec Selection** can be selected by choosing **Custom** from the pull-down menu, allowing an explicit ordered list of codecs to be specified. The **G.711 ULAW 64K** and **G.729(a) 8K CS –ACELP** codecs are selected. Avaya IP Office supports these codecs, which are sent to Windstream, in the Session Description Protocol (SDP) offer, in that order
- Check the **Re-invite Supported** box
- Set **Fax Transport Support** to **G.711** from the pull-down menu. Note: Windstream supported only Fax G.711 pass-through mode during the compliance testing
- Set the **DTMF Support** to **RFC2833** from the pull-down menu. This directs Avaya IP Office to send DTMF tones using SRTP events messages as defined in RFC2833.
- Set **Media Security** as **Preferred**. Check **Same As System** box
- Default values may be used for all other parameters
- Click **OK** to submit the changes



Codec Selection: Custom

Unused:
G.711 ALAW 64K
G.723.1 6K3 MP-MLQ

Selected:
G.711 ULAW 64K
G.729(a) 8K CS-ACELP

Fax Transport Support: G.711

DTMF Support: RFC2833

Media Security: Preferred

Advanced Media Security Options ☑ Same As System

Encryptions ☑ RTP ☑ RTCP

Authentication ☑ RTP ☑ RTCP

Replay Protection

SRTP Window Size: 64

Crypto Suites

☑ SRTP_AES_CM_128_SHA1_80
☑ SRTP_AES_CM_128_SHA1_32

□ VoIP Silence Suppression

□ Local Hold Music

☑ Re-invite Supported

□ Codec Lockdown

□ Allow Direct Media Path

□ Force direct media with phones

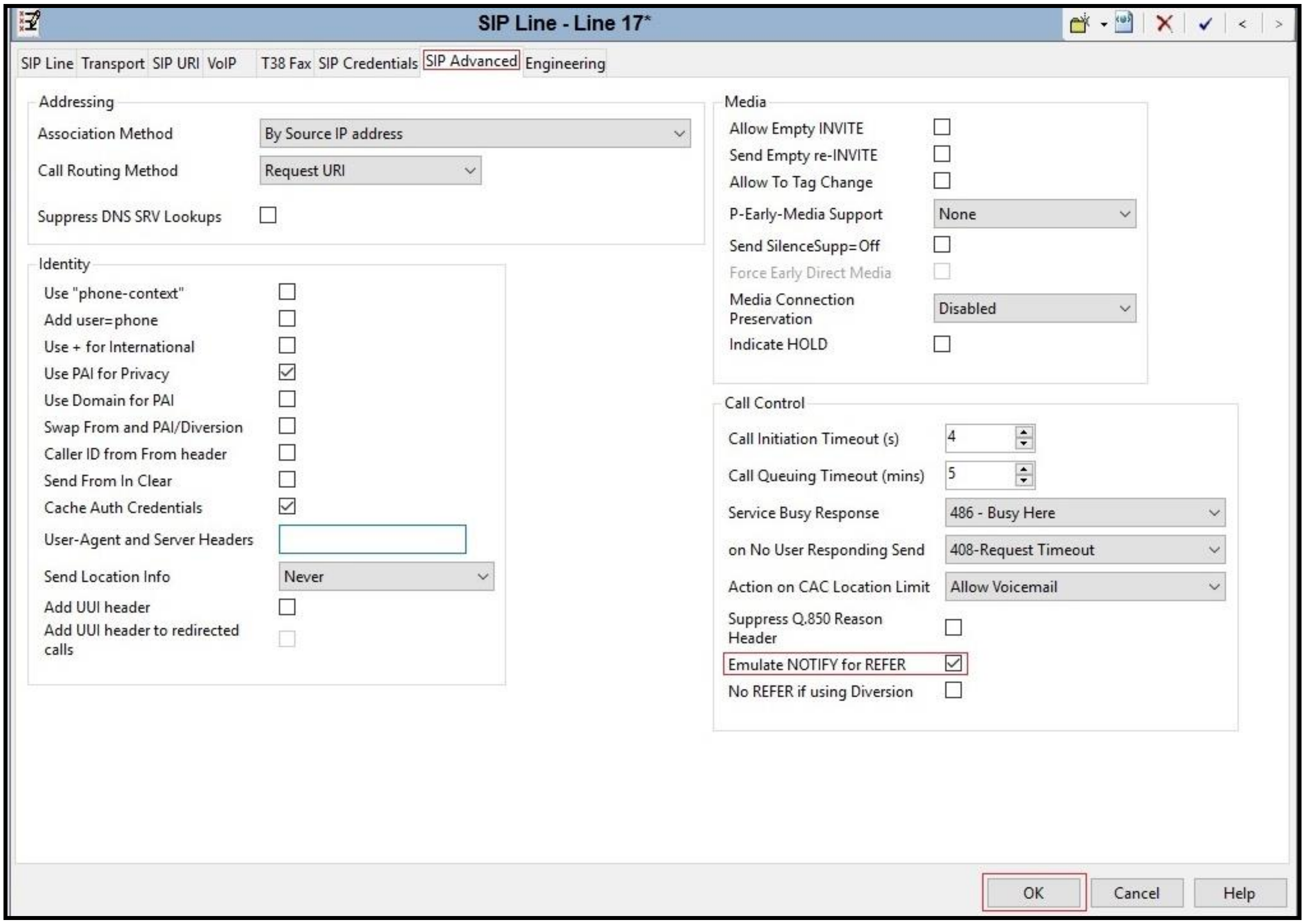
□ PRACK/100rel Supported

□ G.711 Fax ECAN

Figure 18 – SIP Line VoIP Configuration

Select the **SIP Advanced** tab to set the SIP parameters. Set the parameters as shown below:

- Check **Emulate NOTIFY for REFER** option (See observation in **Section** Error! Reference source not found.)
- Default values may be used for all other parameters
- Click **OK** to submit the changes



Addressing

Association Method: By Source IP address

Call Routing Method: Request URI

Suppress DNS SRV Lookups □

Identity

Use "phone-context" □

Add user=phone □

Use + for International □

Use PAI for Privacy ☑

Use Domain for PAI □

Swap From and PAI/Diversion □

Caller ID from From header □

Send From In Clear □

Cache Auth Credentials ☑

User-Agent and Server Headers:

Send Location Info: Never

Add UUI header □

Add UUI header to redirected calls □

Media

Allow Empty INVITE □

Send Empty re-INVITE □

Allow To Tag Change □

P-Early-Media Support: None

Send SilenceSupp=Off □

Force Early Direct Media □

Media Connection Preservation: Disabled

Indicate HOLD □

Call Control

Call Initiation Timeout (s): 4

Call Queuing Timeout (mins): 5

Service Busy Response: 486 - Busy Here

on No User Responding Send: 408-Request Timeout

Action on CAC Location Limit: Allow Voicemail

Suppress Q.850 Reason Header □

Emulate NOTIFY for REFER ☑

No REFER if using Diversion □

Figure 19 – SIP Line SIP Advanced Configuration

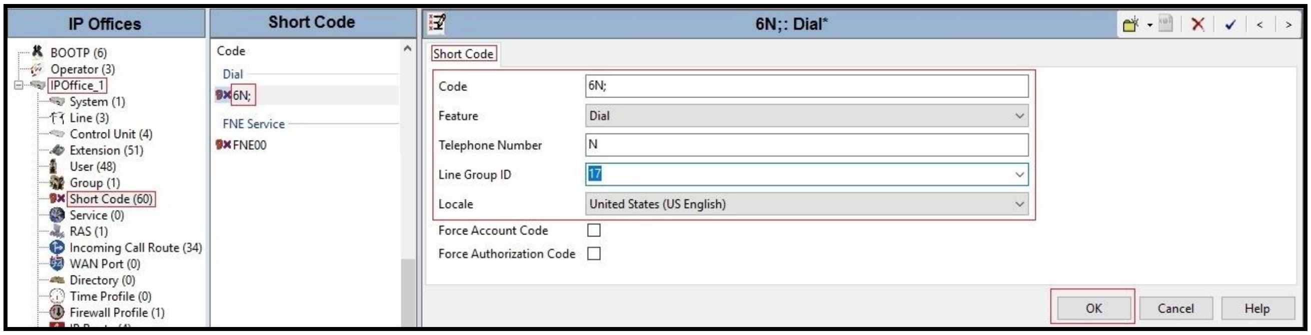
5.7. Outgoing Call Routing

The following section describes the Short Code for outgoing calls to Windstream via Avaya SBCE.

5.7.1. Short Code

Define a short code to route outbound traffic on the SIP line to Windstream via Avaya SBCE. To create a short code, select **Short Code** in the left Navigation Pane, then right-click in the Group Pane and select **New** (not shown). On the **Short Code** tab in the Details Pane, configure the parameters for the new short code to be created. The screen below shows the details of the previously administered “**6N;**” short code used in the test configuration.

- In the **Code** field, enter the dial string which will trigger this short code, followed by a semi-colon. In this case, **6N;**, this short code will be invoked when the user dials 6 followed by any number
- Set **Feature** to **Dial**. This is the action that the short code will perform
- Set **Telephone Number** to **N**. This field is used to construct the Request URI and To headers in the outgoing SIP INVITE message. The value **N** represents the number dialed by the user
- Set the **Line Group ID** to the **Outgoing Group 17** defined on the **SIP URI** tab on the **SIP Line** in **Section 5.6.2**. This short code will use this line group when placing the outbound call
- Set the **Locale** to **United States (US English)**
- Default values may be used for all other parameters
- Click **OK** to submit the changes

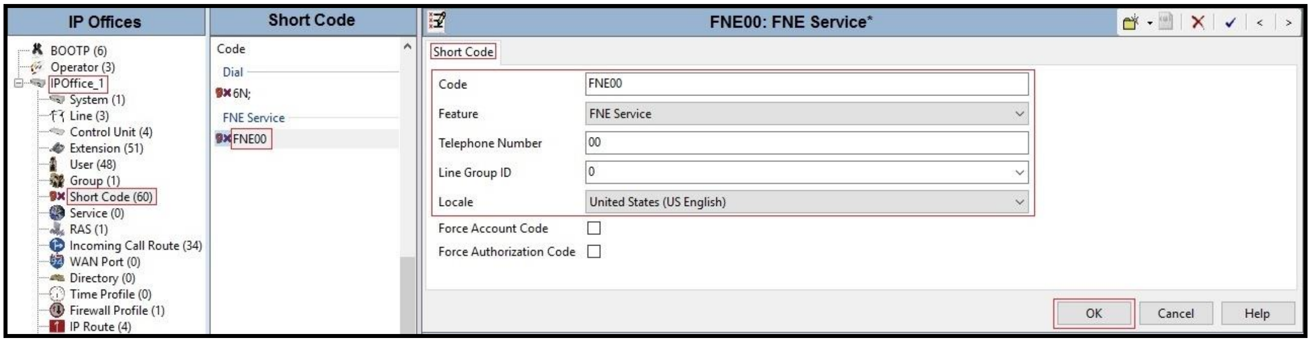


Code	6N;
Feature	Dial
Telephone Number	N
Line Group ID	17
Locale	United States (US English)
Force Account Code	□
Force Authorization Code	□

Figure 20 – Short Code 6N

The feature of incoming calls from mobility extension to idle-appearance FNE (Feature Name Extension) is hosted by Avaya IP Office. The Short Code **FNE00** was configured with following parameters:

- For **Code** field, enter FNE feature code as **FNE00** for dial tone
- Set **Feature** to **FNE Service**
- Set **Telephone Number** to **00**
- Set **Line Group ID** to **0**
- Set the **Locale** to **United States (US English)**
- Default values may be used for other parameters
- Click **OK** to submit the changes



FNE00: FNE Service*

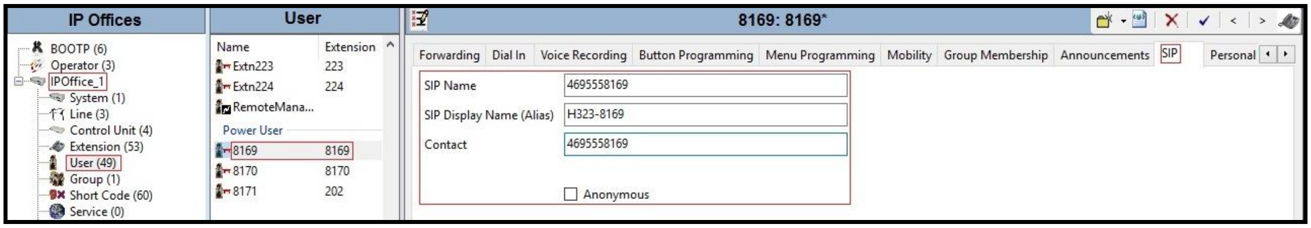
Code	FNE00
Feature	FNE Service
Telephone Number	00
Line Group ID	0
Locale	United States (US English)
Force Account Code	□
Force Authorization Code	□

Figure 21 – Short Code FNE

5.8. User

Configure the SIP parameters for each user that will be placing and receiving calls via the SIP Line defined in **Section 5.6**. To configure these settings, first select **User** in the left Navigation Pane, then select the name of the user to be modified in the center Group Pane. In the example below, the name of the user is **8169**. Select the **SIP** tab in the Details pane.

The values entered for the **SIP Name** and **Contact** fields are used as the user part of the SIP URI in the From and Contact headers accordingly for outgoing SIP trunk calls. They also allow matching of the SIP URI for incoming calls without having to enter this number as an explicit SIP URI for the SIP line. The example below shows the settings for user **8169**. The **SIP Name** and **Contact** are set to one of the DID numbers assigned to the enterprise provided by Windstream. The **SIP Display Name (Alias)** parameter can optionally be configured with a descriptive name. If all calls involving this user and a SIP Line should be considered private, then the **Anonymous** box may be checked to withhold the user's information from the network.



Name	Extension
Extn223	223
Extn224	224
RemoteMana...	
Power User	
8169	8169
8170	8170
8171	202

SIP Name: 4695558169

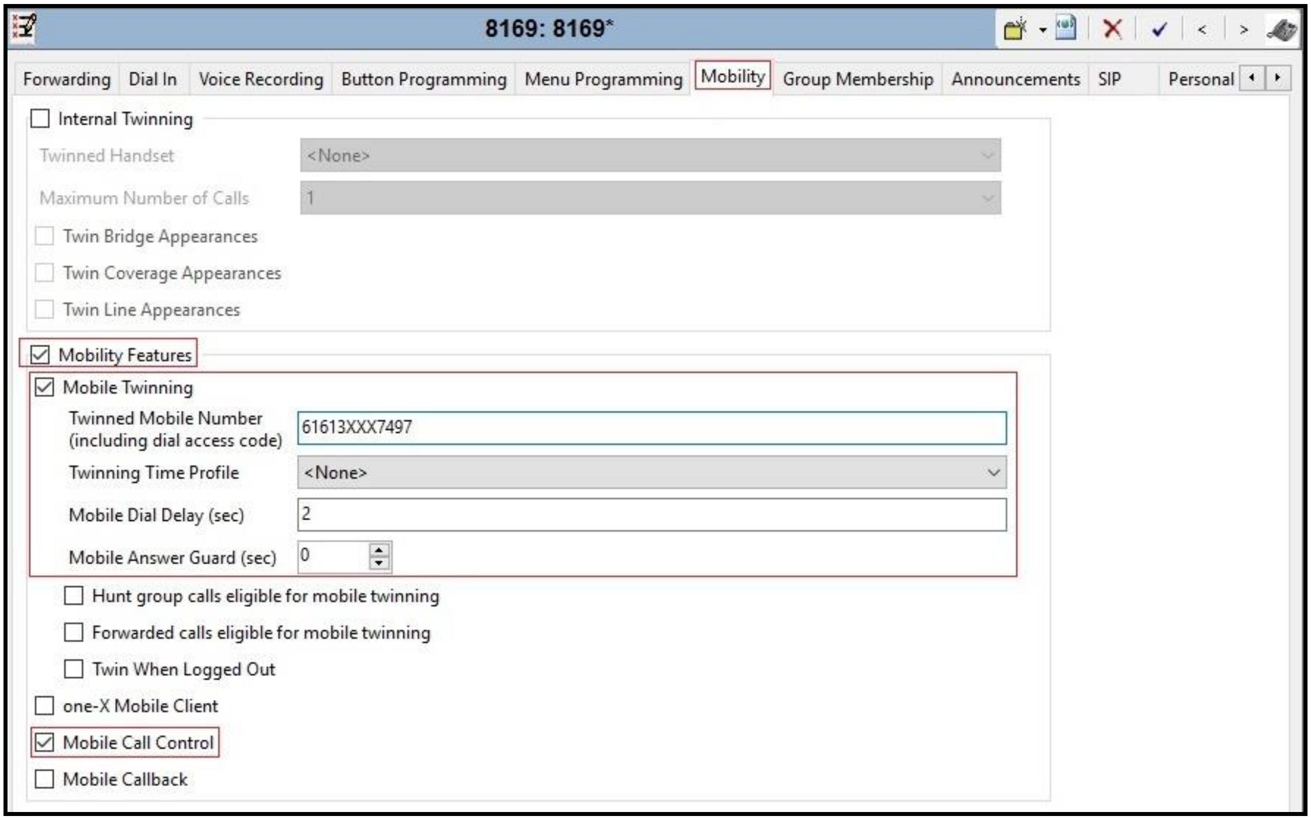
SIP Display Name (Alias): H323-8169

Contact: 4695558169

☐ Anonymous

Figure 22 – User Configuration

One of the H.323 IP Deskphones at the enterprise site uses the Mobile Twinning feature. The following screen shows the **Mobility** tab for User 8169. The **Mobility Features** and **Mobile Twinning** boxes are checked. The **Twinned Mobile Number** field is configured with the number to dial to reach the twinned mobile telephone, in this case **61613XXX7497**. Check **Mobile Call Control** to allow incoming calls from mobility extension to access FNE00 (defined in **Section 5.7.1**). Other options can be set according to customer requirements.



☐ Internal Twinning

Twinned Handset: <None>

Maximum Number of Calls: 1

☐ Twin Bridge Appearances

☐ Twin Coverage Appearances

☐ Twin Line Appearances

☑ Mobility Features

☑ Mobile Twinning

Twinned Mobile Number (including dial access code): 61613XXX7497

Twinning Time Profile: <None>

Mobile Dial Delay (sec): 2

Mobile Answer Guard (sec): 0

☐ Hunt group calls eligible for mobile twinning

☐ Forwarded calls eligible for mobile twinning

☐ Twin When Logged Out

☐ one-X Mobile Client

☑ Mobile Call Control

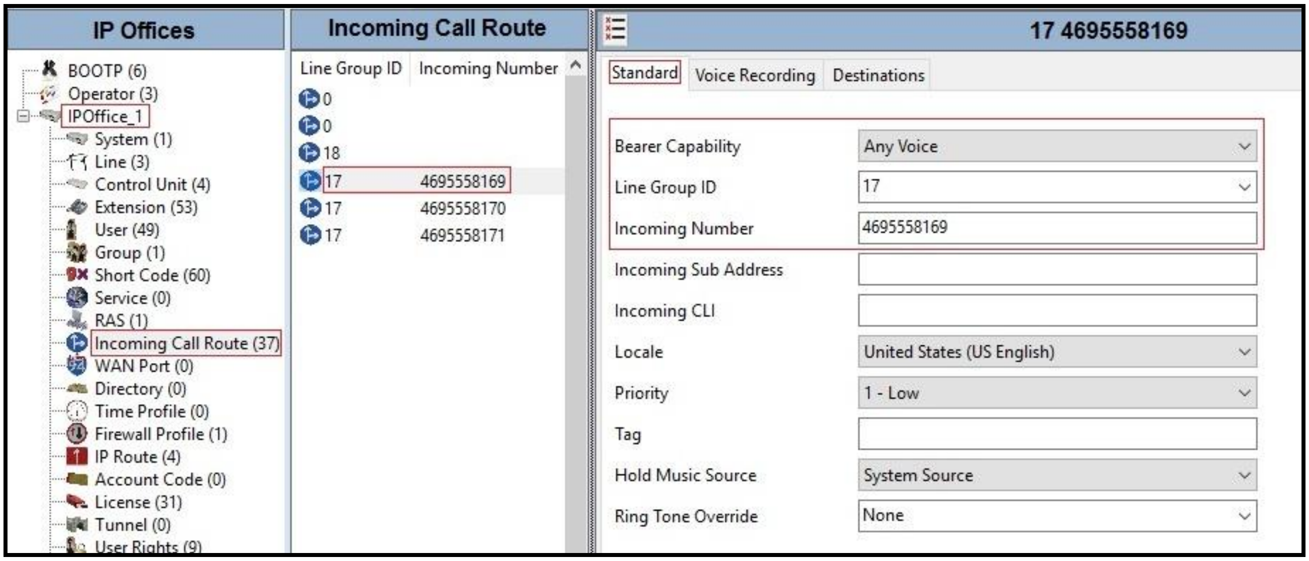
☐ Mobile Callback

Figure 23 – Mobility Configuration for User

5.9. Incoming Call Route

An Incoming Call Route maps an inbound DID number on a specific line to an internal extension. This procedure should be repeated for each DID number provided by service provider. To create an incoming call route, select **Incoming Call Route** in the left Navigation Pane, then right-click in the center Group Pane and select **New** (not shown). On the **Standard** tab of the Details Pane, enter the parameters as shown below:

- Set the **Bearer Capability** to **Any Voice**.
- Set the **Line Group ID** to the **Incoming Group 17** defined on the **SIP URI** tab on the **SIP Line** in **Section 5.6.2**.
- Set the **Incoming Number** to the incoming DID number on which this route should match.
- Default values can be used for all other fields.

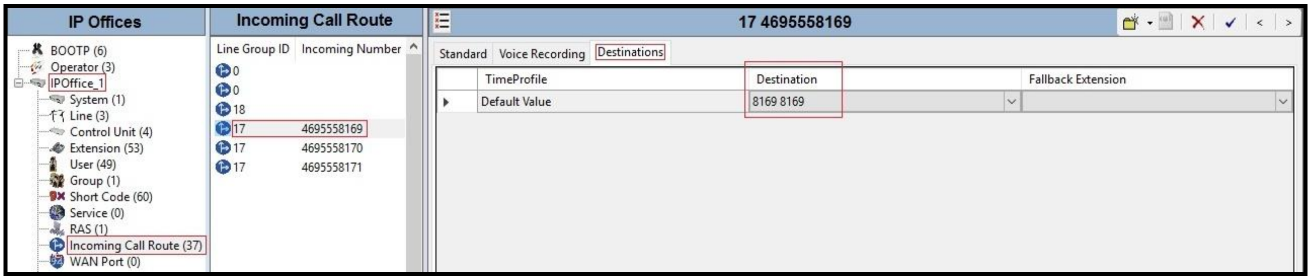


Line Group ID	Incoming Number
0	
0	
18	
17	4695558169
17	4695558170
17	4695558171

Bearer Capability	Any Voice
Line Group ID	17
Incoming Number	4695558169
Incoming Sub Address	
Incoming CLI	
Locale	United States (US English)
Priority	1 - Low
Tag	
Hold Music Source	System Source
Ring Tone Override	None

Figure 24 – Incoming Call Route Configuration

On the **Destination** tab, select the destination extension from the pull-down menu of the **Destination** field. In this example, incoming calls to **4695558169** on line 17 are routed to **Destination 8169 8169** as below screenshot:

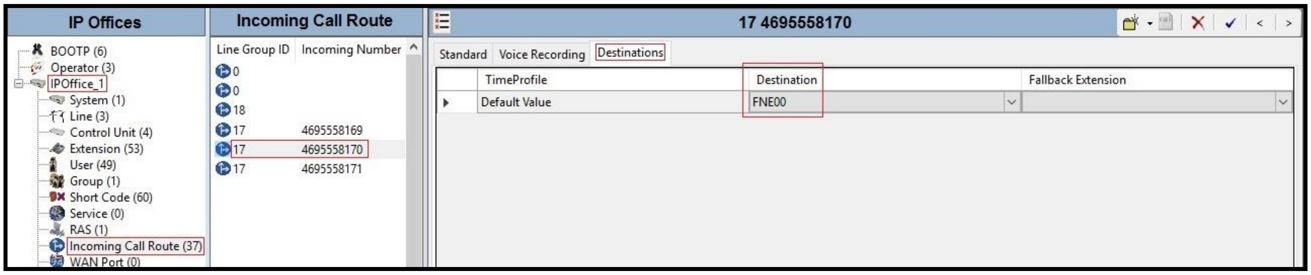


Line Group ID	Incoming Number
0	
0	
18	
17	4695558169
17	4695558170
17	4695558171

TimeProfile	Destination	Fallback Extension
Default Value	8169 8169	

Figure 25 – Incoming Call Route for Destination 8169

For Feature Name Extension Service testing purpose, the incoming calls to DID number **4695558170** were configured to access **FNE00**. The **Destination** was appropriately defined as **FNE00** as below screenshot:

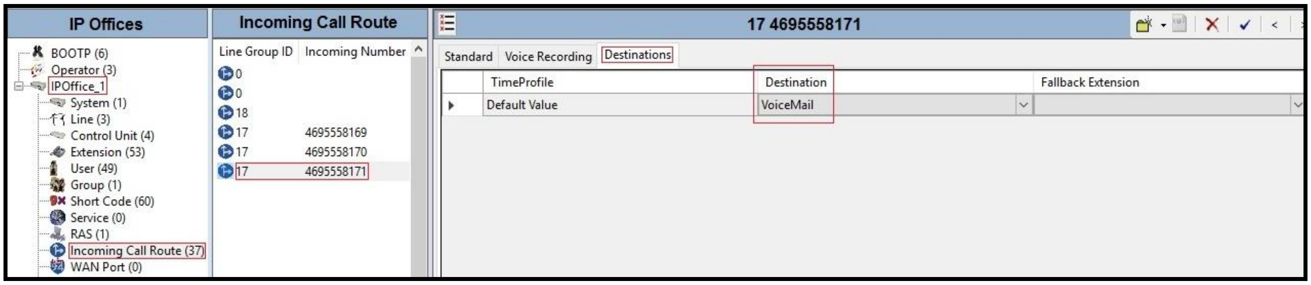


Line Group ID	Incoming Number
0	
0	
18	
17	4695558169
17	4695558170
17	4695558171

	TimeProfile	Destination	Fallback Extension
▸	Default Value	FNE00	

Figure 26 – Incoming Call Route for Destination FNE

For Voice Mail testing purpose, the incoming calls to DID number **4695558171** were configured to access **VoiceMail**. The **Destination** was appropriately defined as **VoiceMail** as below screenshot:



Line Group ID	Incoming Number
0	
0	
18	
17	4695558169
17	4695558170
17	4695558171

	TimeProfile	Destination	Fallback Extension
▸	Default Value	VoiceMail	

Figure 27 – Incoming Call Route for Destination VoiceMail

5.10. Save Configuration

Navigate to **File → Save Configuration** in the menu bar at the top of the screen to save the configuration performed in the preceding sections.

6. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of Avaya SBCE necessary for interoperability with the Avaya IP Office and Windstream SIP Trunk Service.

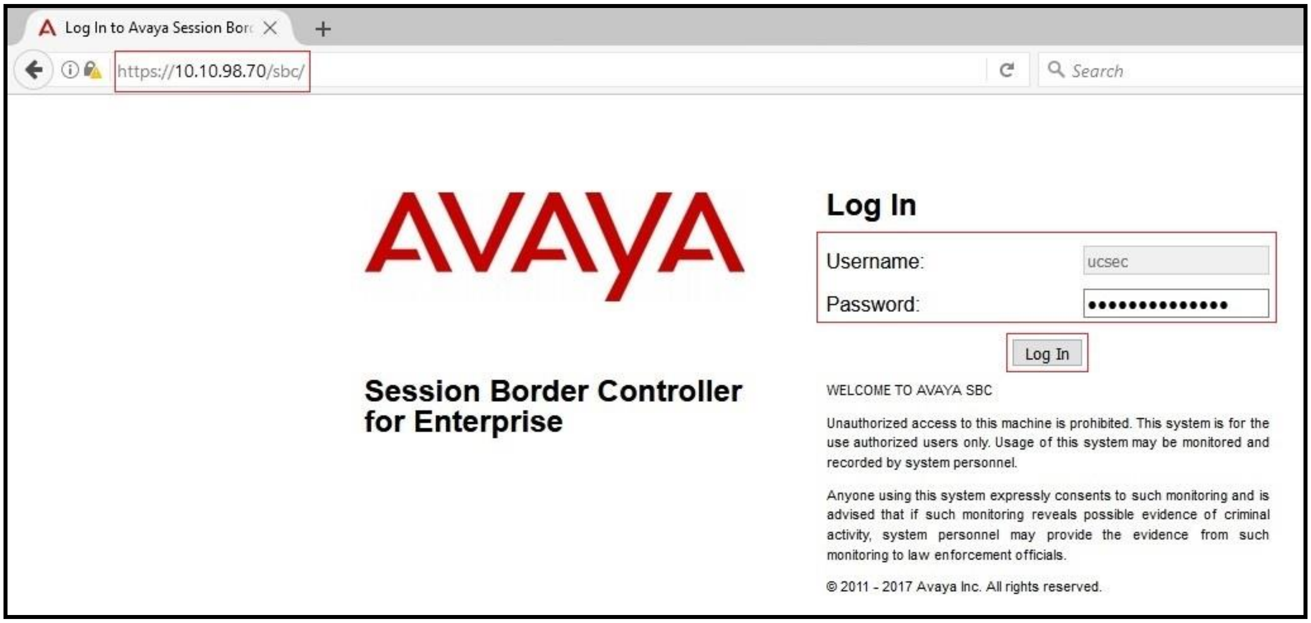
Avaya elements reside on the Private side and the Windstream SIP Trunk Service resides on the Public side of the network, as illustrated in **Figure 1**.

Note: The following section assumes that Avaya SBCE has been installed and that network connectivity exists between the systems. For more information on Avaya SBCE, see relevant product documentation references in **Section 10** of these Application Notes.

6.1. Log in to the Avaya SBCE

Access the web interface by typing "**https://x.x.x.x/sbc/**" (where x.x.x.x is the management IP address of the Avaya SBCE).

Enter the **Username** and **Password**.


Log In to Avaya Session Bor
Search
AVAYA
Session Border Controller for Enterprise
Log In
Log In

https://10.10.98.70/sbc/

Username: ucsec

Password: ••••••••••••••

WELCOME TO AVAYA SBC

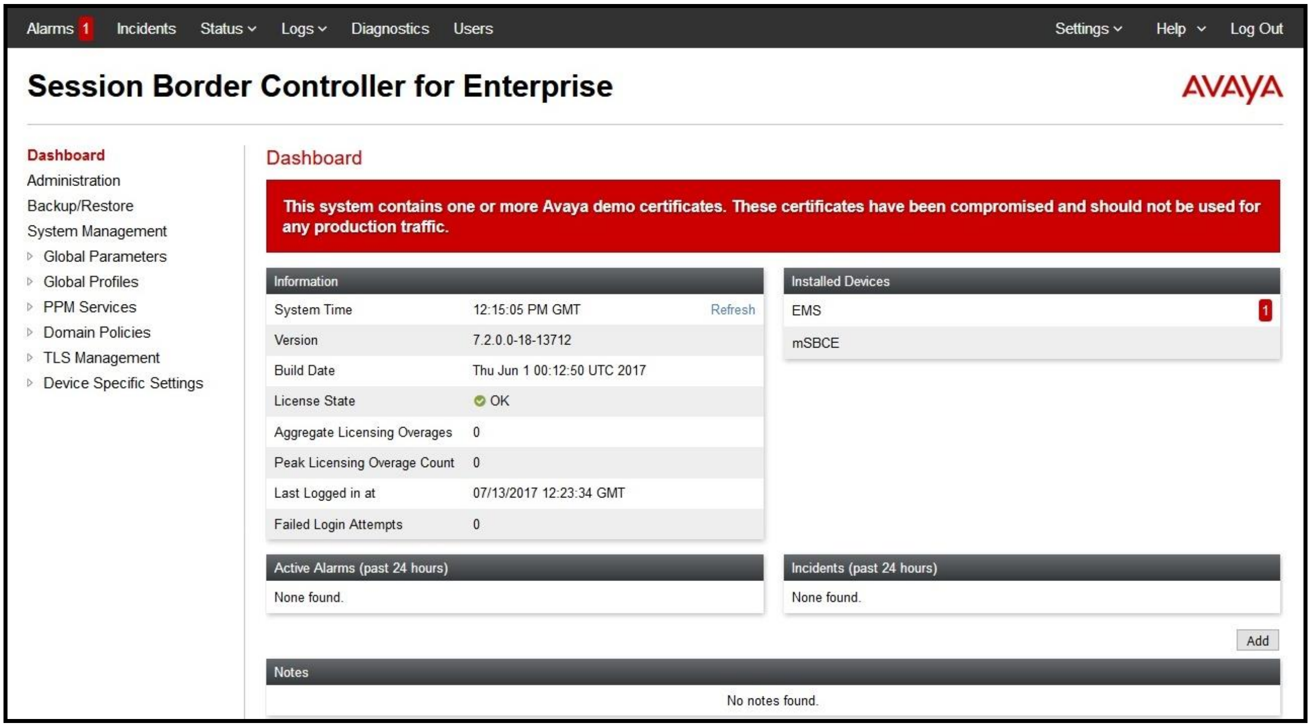
Unauthorized access to this machine is prohibited. This system is for the use authorized users only. Usage of this system may be monitored and recorded by system personnel.

Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence from such monitoring to law enforcement officials.

© 2011 - 2017 Avaya Inc. All rights reserved.

Figure 28 – Avaya SBCE Login

The **Dashboard** main page will appear as shown below.



Session Border Controller for Enterprise

Dashboard

This system contains one or more Avaya demo certificates. These certificates have been compromised and should not be used for any production traffic.

Information	
System Time	12:15:05 PM GMT Refresh
Version	7.2.0.0-18-13712
Build Date	Thu Jun 1 00:12:50 UTC 2017
License State	✓ OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	07/13/2017 12:23:34 GMT
Failed Login Attempts	0

Installed Devices	
EMS	1
mSBCE	

Active Alarms (past 24 hours)

None found.

Incidents (past 24 hours)

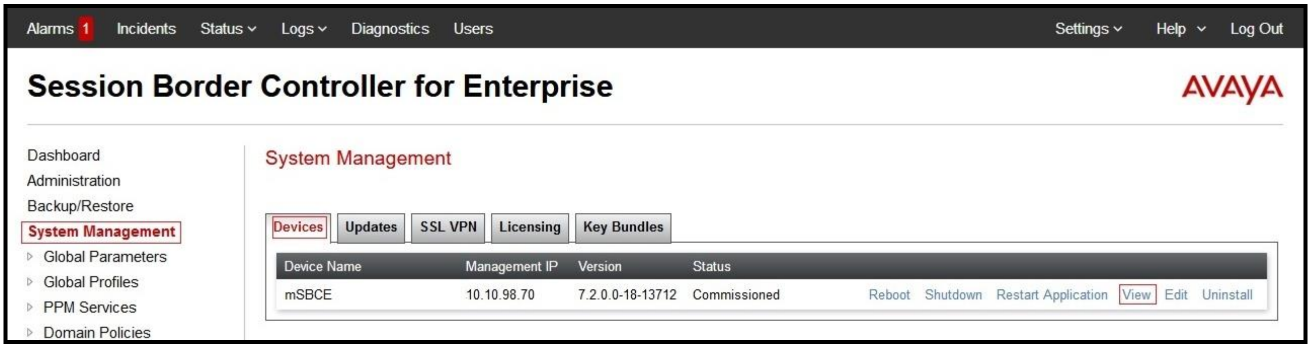
None found.

Notes

No notes found.

Figure 29 - Avaya SBCE Dashboard

To view system information that has been configured during installation, navigate to **System Management**. A list of installed devices is shown in the right pane. In the compliance test, a single Device Name **mSBCE** was already added. To view the configuration of this device, click **View** as shown in the screenshot below.



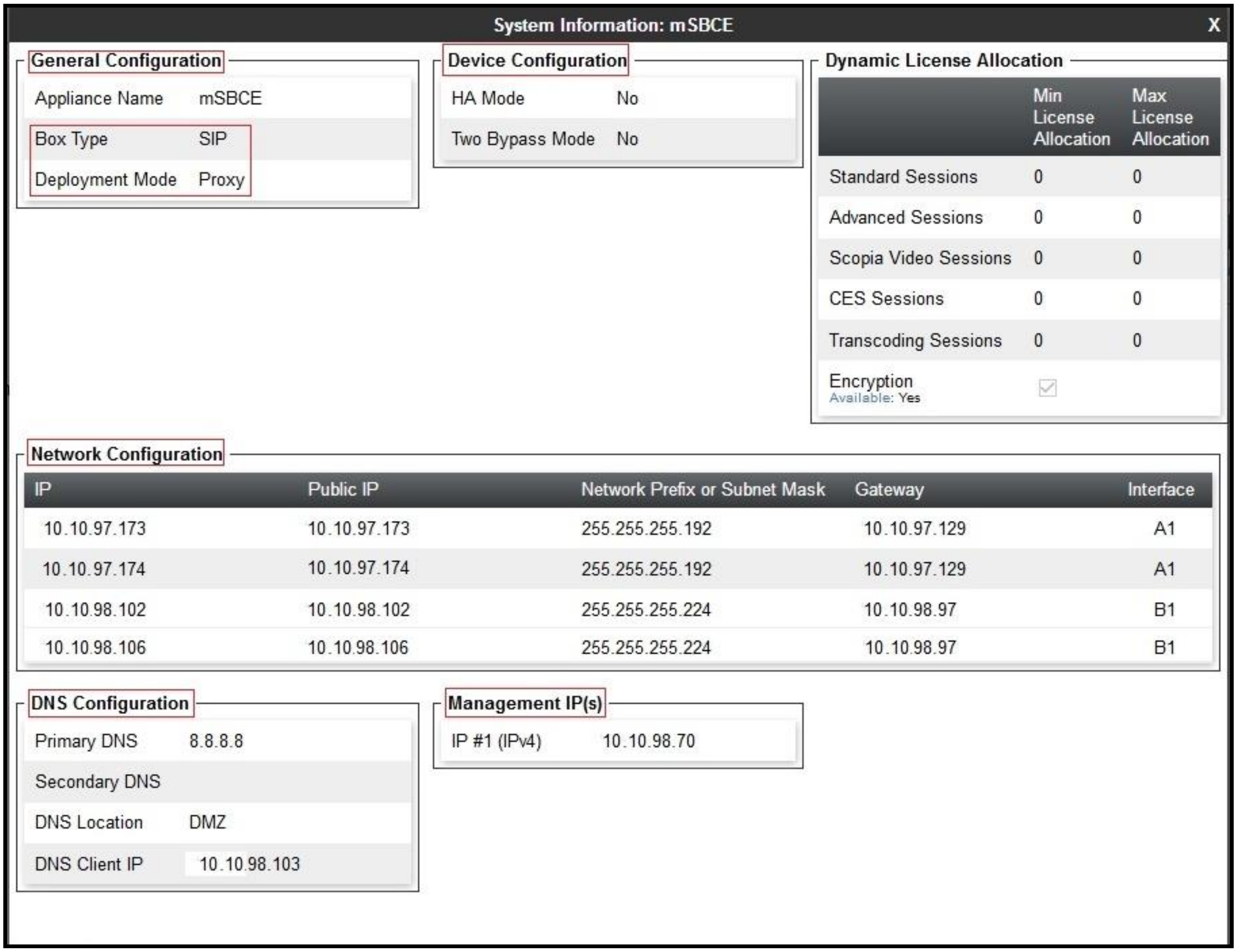
Session Border Controller for Enterprise

System Management

Device Name	Management IP	Version	Status	
mSBCE	10.10.98.70	7.2.0.0-18-13712	Commissioned	Reboot Shutdown Restart Application View Edit Uninstall

Figure 30 - Avaya SBCE System Management

The **System Information** screen shows **General Configuration**, **Device Configuration**, **Network Configuration**, **DNS Configuration** and **Management IP(s)** information provided during installation and corresponds to **Figure 1**. The **Box Type** was set to **SIP** and the **Deployment Mode** was set to **Proxy**.



System Information: mSBCE

General Configuration

Appliance Name	mSBCE
Box Type	SIP
Deployment Mode	Proxy

Device Configuration

HA Mode	No
Two Bypass Mode	No

Dynamic License Allocation

	Min License Allocation	Max License Allocation
Standard Sessions	0	0
Advanced Sessions	0	0
Scopia Video Sessions	0	0
CES Sessions	0	0
Transcoding Sessions	0	0
Encryption Available: Yes	☑	

Network Configuration

IP	Public IP	Network Prefix or Subnet Mask	Gateway	Interface
10.10.97.173	10.10.97.173	255.255.255.192	10.10.97.129	A1
10.10.97.174	10.10.97.174	255.255.255.192	10.10.97.129	A1
10.10.98.102	10.10.98.102	255.255.255.224	10.10.98.97	B1
10.10.98.106	10.10.98.106	255.255.255.224	10.10.98.97	B1

DNS Configuration

Primary DNS	8.8.8.8
Secondary DNS	
DNS Location	DMZ
DNS Client IP	10.10.98.103

Management IP(s)

IP #1 (IPv4)	10.10.98.70

Figure 31 - Avaya SBCE System Information

6.2. Global Profiles

When selected, Global Profiles allows for configuration of parameters across all Avaya SBCE appliances.

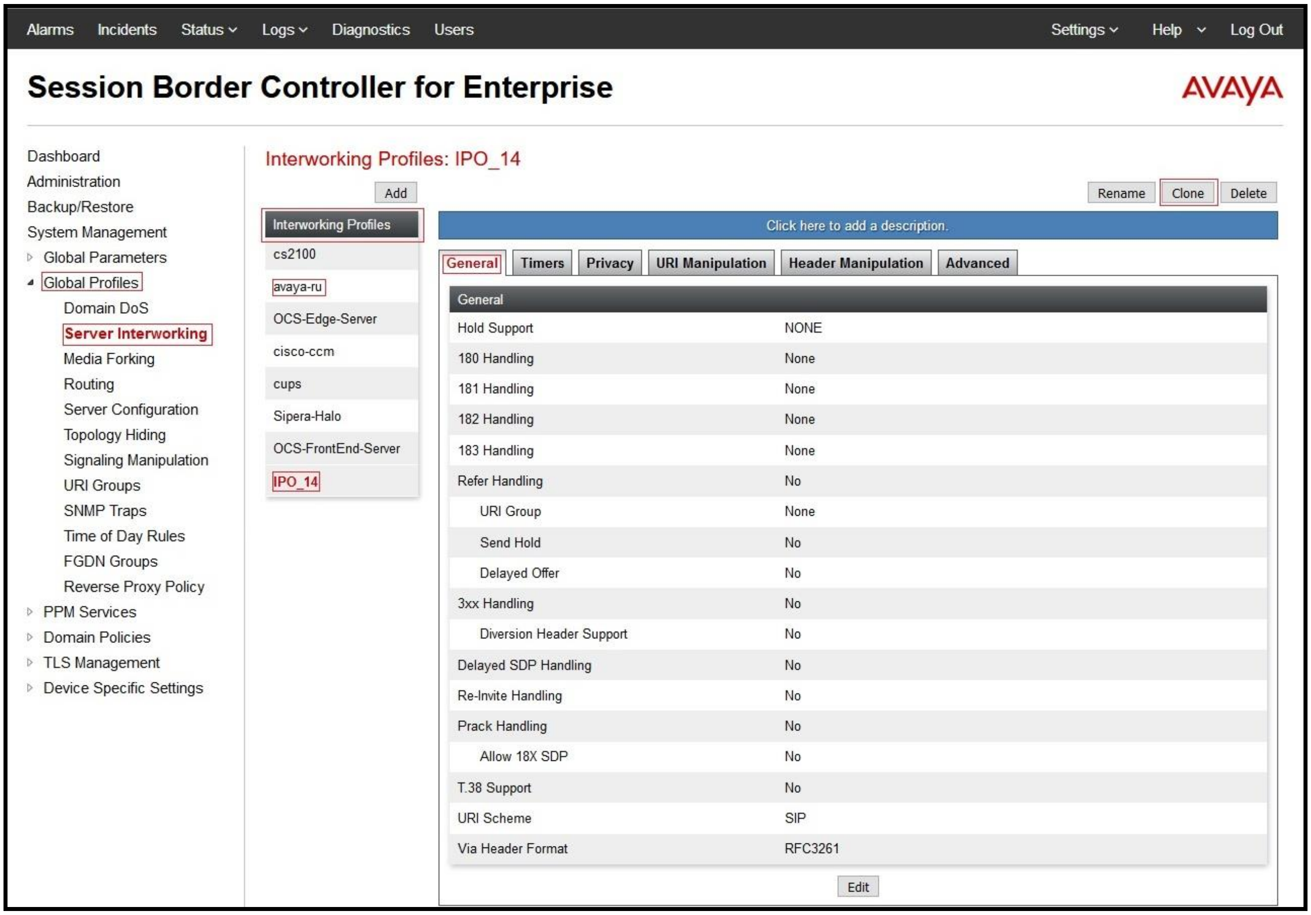
6.2.1. Configure Server Interworking Profile – Avaya IP Office

Server Interworking profile allows administrator to configure and manage various SIP call server-specific capabilities such as call hold, 180 handling, etc.

From the menu on the left-hand side, select **Global Profiles** → **Server Interworking**

- Select **avaya-ru** in **Interworking Profiles**
- Click **Clone**
- Enter **Clone Name**: **IPO_14** and click **Finish** (not shown)

The following screen shows that Avaya IP Office server interworking profile (named: **IPO_14**) was added.



General	
Hold Support	NONE
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
Send Hold	No
Delayed Offer	No
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
Prack Handling	No
Allow 18X SDP	No
T.38 Support	No
URI Scheme	SIP
Via Header Format	RFC3261

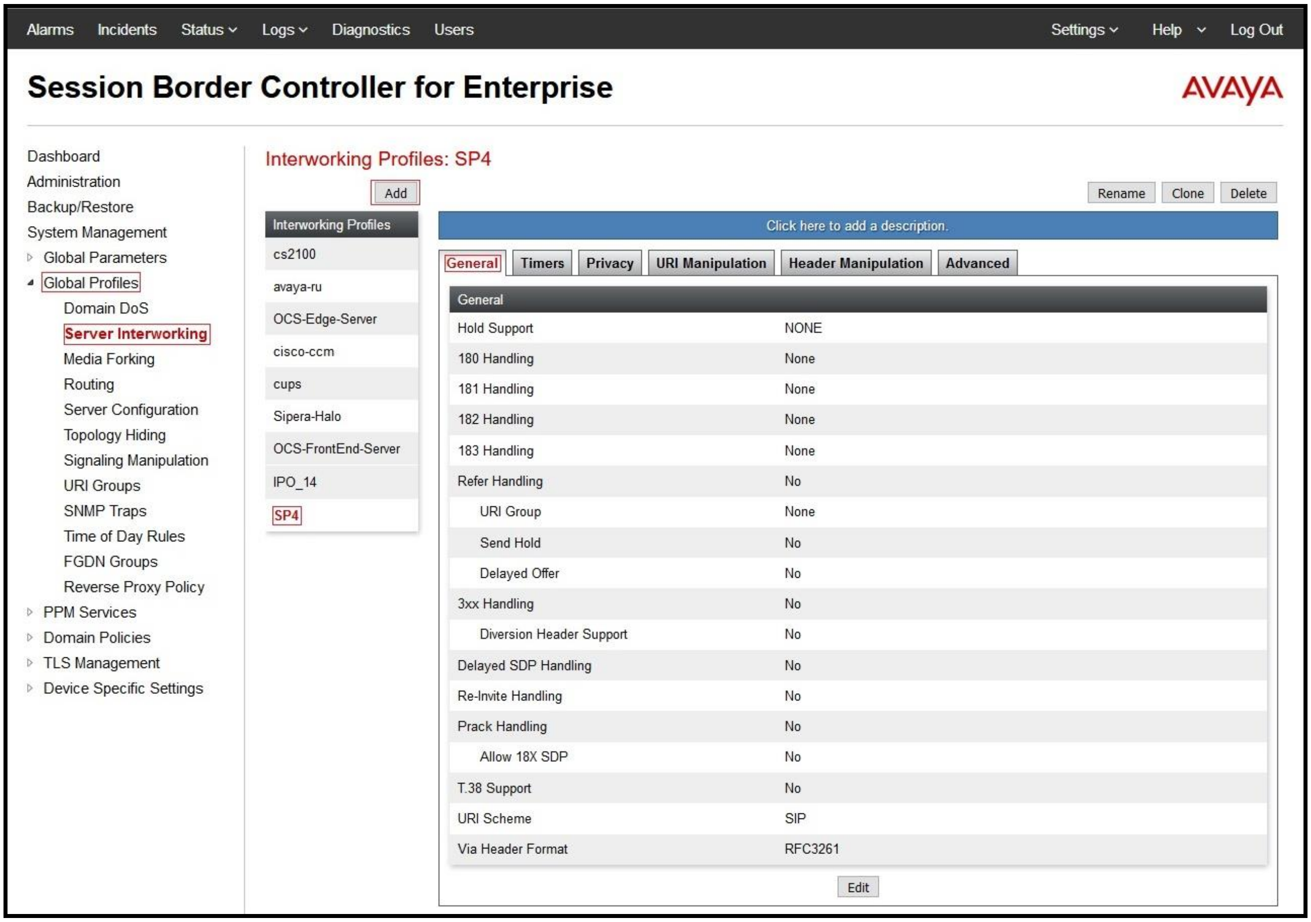
Figure 32 - Server Interworking – Avaya

6.2.2. Configure Server Interworking Profile – Windstream

From the menu on the left-hand side, select **Global Profiles → Server Interworking → Add**

- Enter **Profile Name**: **SP4** (not shown)
- Click **Next** button to leave all options at default
- Click **Finish** (not shown)

The following screen shows that Windstream server interworking profile (named: **SP4**) was added.



General	
Hold Support	NONE
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
Send Hold	No
Delayed Offer	No
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
Prack Handling	No
Allow 18X SDP	No
T.38 Support	No
URI Scheme	SIP
Via Header Format	RFC3261

Figure 33 - Server Interworking – Windstream

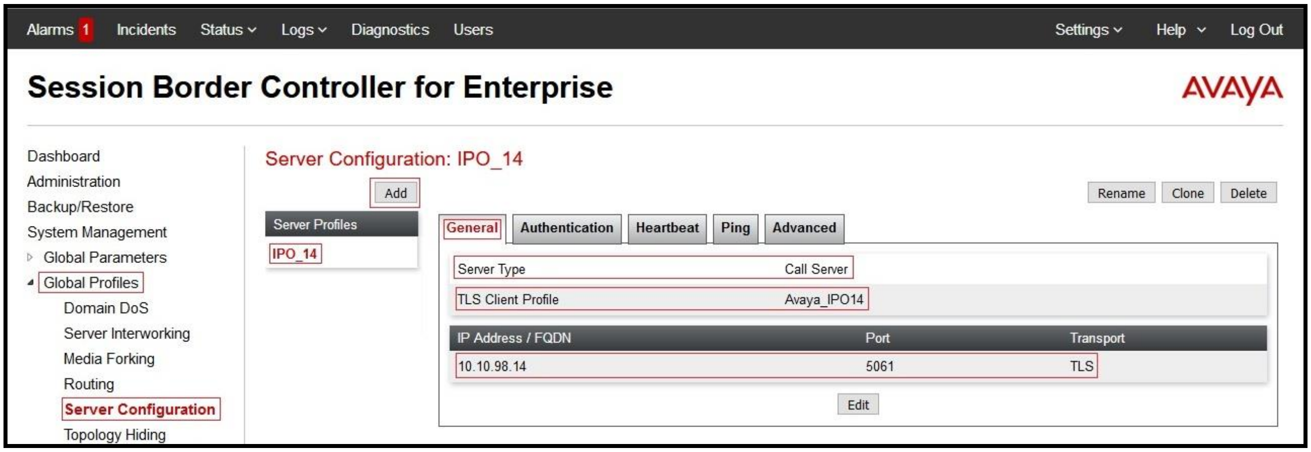
6.2.3. Configure Server – Avaya IP Office

The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together, these tabs allow one to configure and manage various SIP call server-specific parameters such as TLS port assignment, IP Server type, heartbeat signaling parameters and some advanced options.

From the menu on the left-hand side, select **Global Profiles → Server Configuration → Add**

Enter **Profile Name**: **IPO_14** (not shown).
On **General** tab, enter the following:

- **Server Type**: Select **Call Server**
- **TLS Client Profile**: Select **Avaya_IPO14**. Note: During the compliance test in the lab environment, demo certificates are used and are not recommended for production use. Consult the appropriate Avaya product documentation for further information regarding security certificate and encryption capabilities supported by Avaya product
- **IP Address/FQDN**: **10.10.98.14** (Avaya IP Office IP LAN2 port IP address)
- **Port**: **5061**
- **Transport**: **TLS**
- Click **Finish** (not shown)



Server Configuration: IPO_14

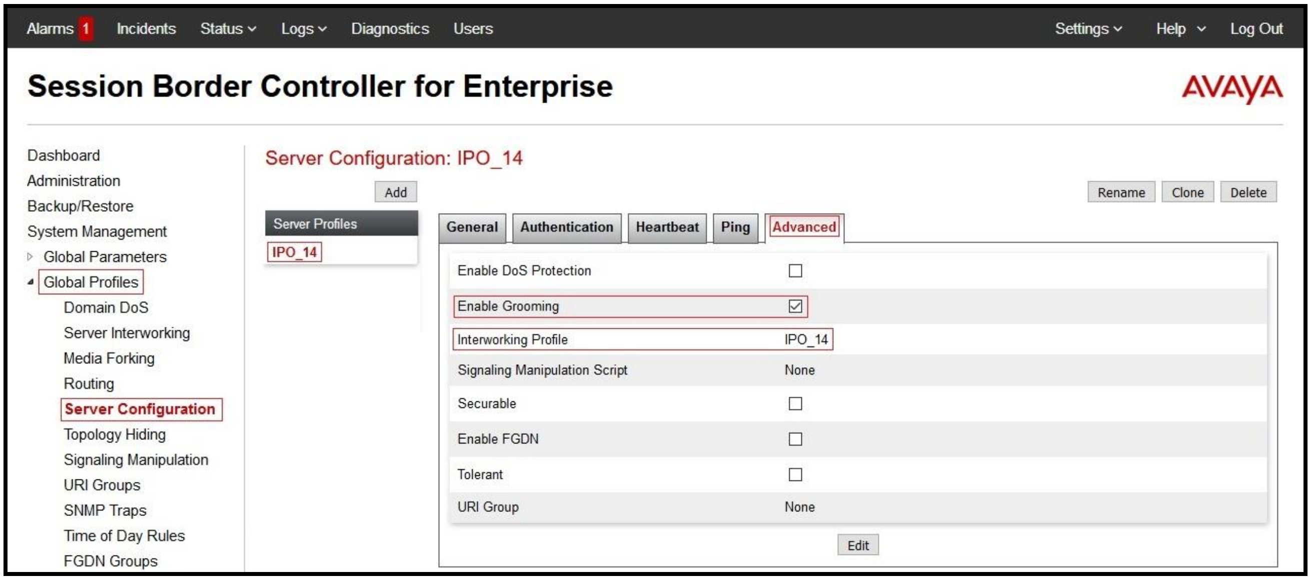
Server Type	Call Server
TLS Client Profile	Avaya_IPO14

IP Address / FQDN	Port	Transport
10.10.98.14	5061	TLS

Figure 34 – Avaya Server Configuration – General

On the **Advanced** tab:

- Check **Enable Grooming** box
- Select **IPO_14** for **Interworking Profile** (see **Section 6.2.1**)
- Click **Finish** (not shown)



Enable DoS Protection	□
Enable Grooming	☑
Interworking Profile	IPO_14
Signaling Manipulation Script	None
Securable	□
Enable FGDN	□
Tolerant	□
URI Group	None

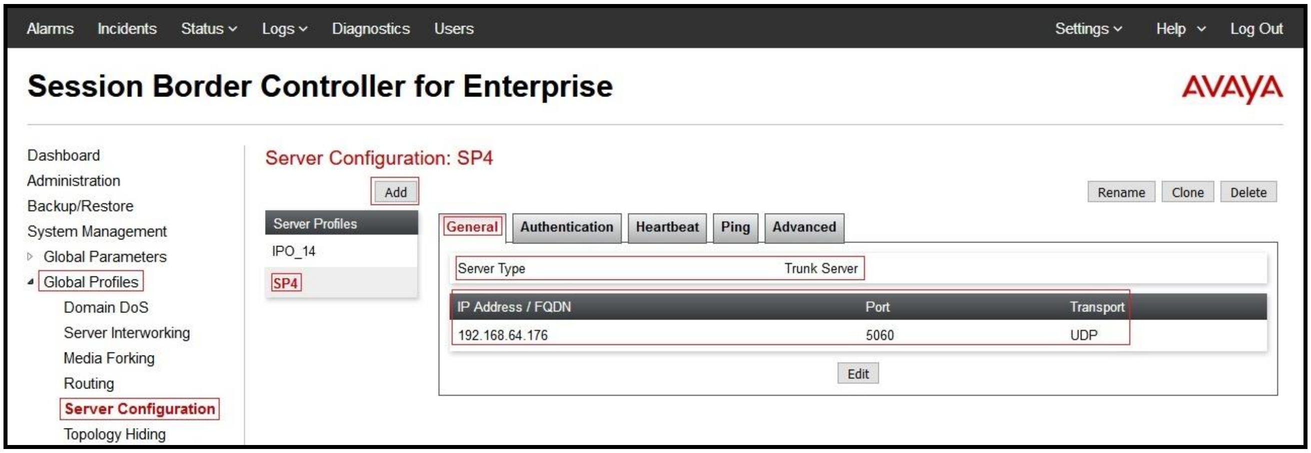
Figure 35 – Avaya Server Configuration – Advanced

6.2.4. Configure Server – Windstream

From the menu on the left-hand side, select **Global Profiles → Server Configuration → Add**

Enter **Profile Name**: **SP4** (not shown)
On **General** tab, enter the following:

- **Server Type**: Select **Trunk Server**
- Add **IP Address/FQDN**: **192.168.64.176** (Windstream Signaling Server IP address)
- **Port**: **5060**
- **Transport**: **UDP**
- Click **Finish** (not shown)



Server Configuration: SP4

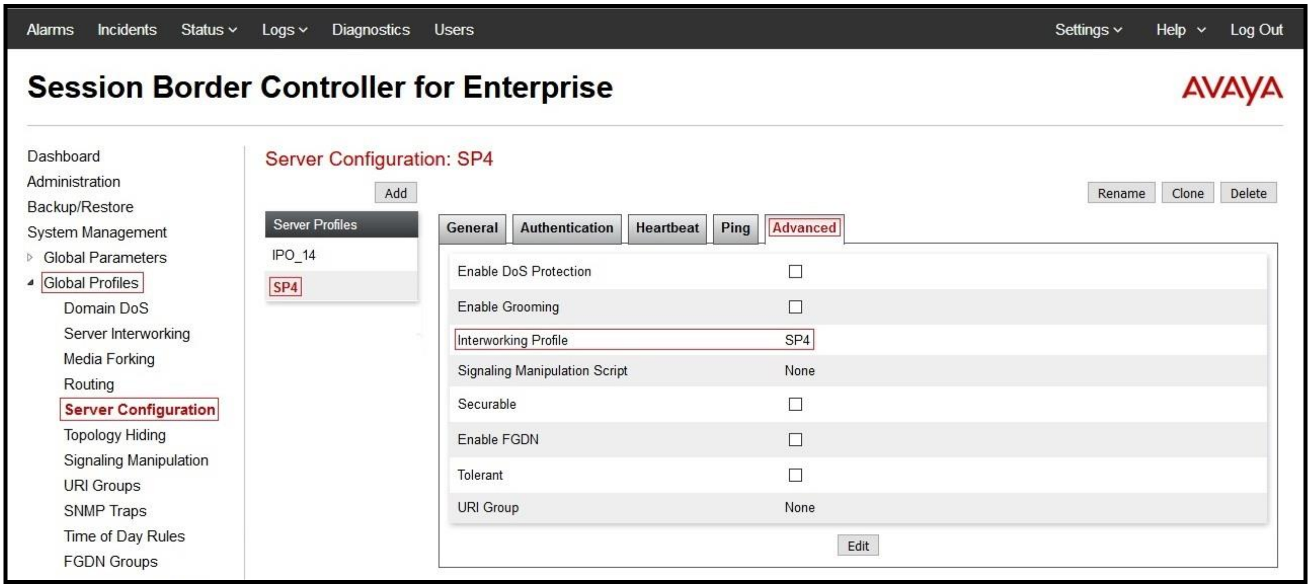
Server Type	Trunk Server

IP Address / FQDN	Port	Transport
192.168.64.176	5060	UDP

Figure 36 - Windstream Server Configuration – General

On the **Advanced** tab, enter the following:

- **Interworking Profile**: Select **SP4** (see **Section 6.2.2**)
- Click **Finish** (not shown)



Server Configuration: SP4

Enable DoS Protection	□
Enable Grooming	□
Interworking Profile	SP4
Signaling Manipulation Script	None
Securable	□
Enable FGDN	□
Tolerant	□
URI Group	None

Figure 37 - Windstream Server Configuration – Advanced

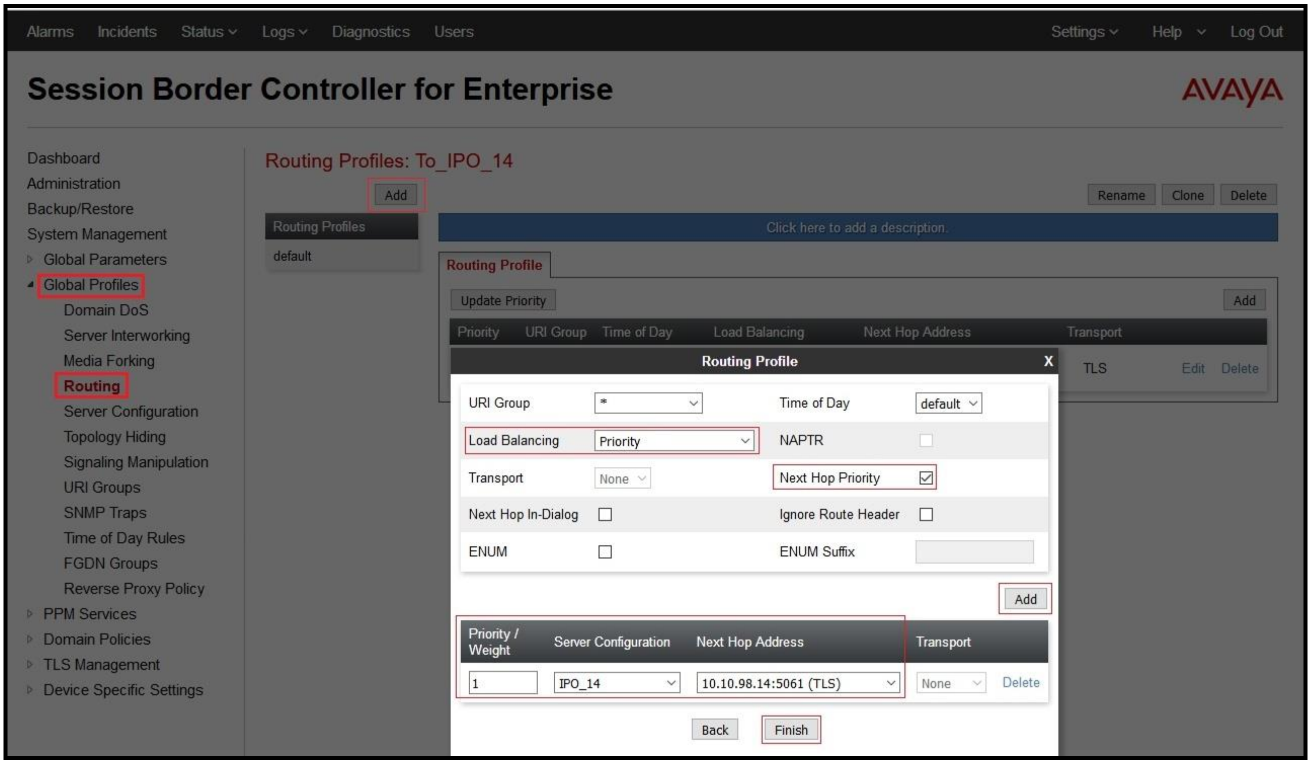
6.2.5. Configure Routing – Avaya IP Office

Routing profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby ascertain which security features will be applied to those packets. Parameters defined by Routing Profiles include packet transport settings, name server addresses and resolution methods, next hop routing information, and packet transport types.

From the menu on the left-hand side, select **Global Profiles → Routing** and click **Add** as highlighted below.

Enter **Profile Name**: **To_IPO_14** and click **Next** button (not shown)

- Select **Load Balancing**: **Priority**
- Check **Next Hop Priority**
- Click **Add** button to add a Next-Hop Address
- **Priority/Weight**: **1**
- **Server Configuration**: **IPO_14** (see **Section 6.2.3**). This selection will automatically populate the **Next Hop Address** field with **10.10.98.14:5061 (TLS)** (Avaya IP Office LAN2 port IP address)
- Click **Finish**



URI Group	*	Time of Day	default
Load Balancing	Priority	NAPTR	□
Transport	None	Next Hop Priority	☑
Next Hop In-Dialog	□	Ignore Route Header	□
ENUM	□	ENUM Suffix	

Priority / Weight	Server Configuration	Next Hop Address	Transport	
1	IPO_14	10.10.98.14:5061 (TLS)	None	Delete

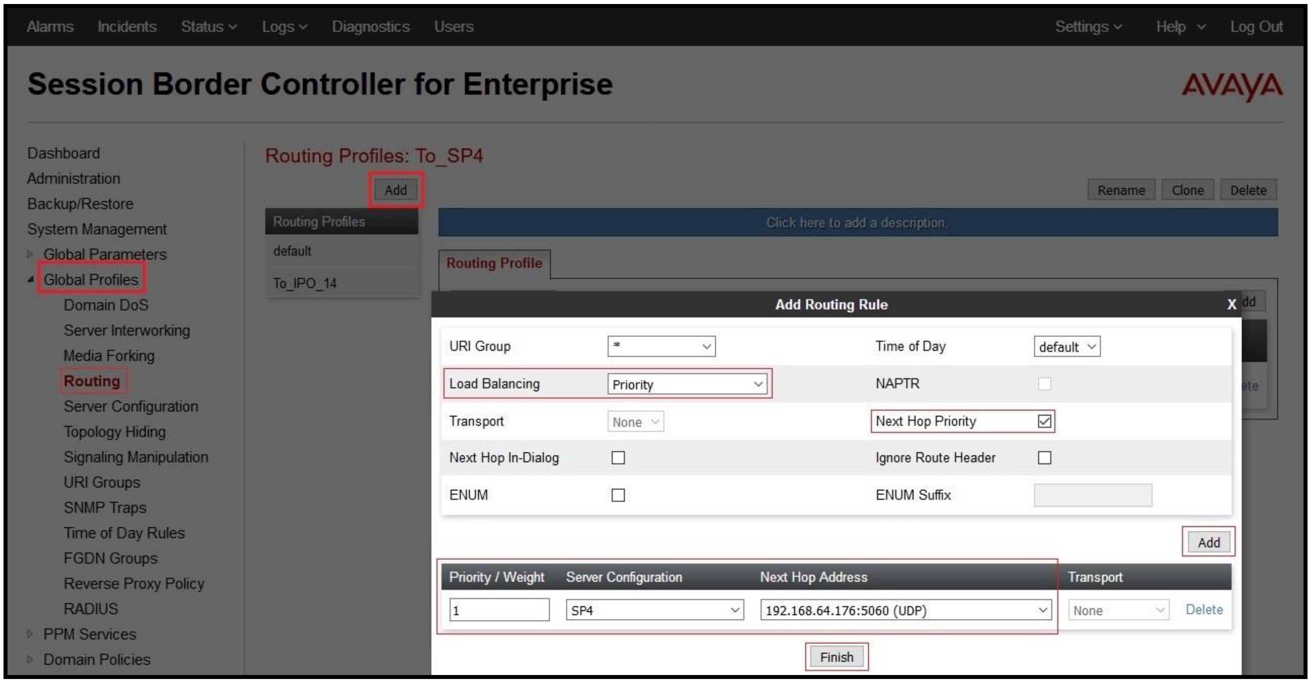
Figure 38 - Routing to Avaya IP Office

6.2.6. Configure Routing – Windstream

From the menu on the left-hand side, select **Global Profiles** → **Routing** and click **Add** as highlighted below.

Enter **Profile Name**: **To_SP4** (not shown)

- **Load Balancing**: **Priority**
- Check **Next Hop Priority**
- Click **Add** button to add a Next-Hop Address
  - **Priority/Weight**: **1**, **Server Configuration**: **SP4** (see **Section 6.2.4**). This selection will automatically populate the **Next Hop Address** field drop-down menu. Select **192.168.64.176:5060 (UDP)** (Windstream Signaling IP Address)
- Click **Finish**



Routing Profiles: To_SP4

URI Group	*	Time of Day	default
Load Balancing	Priority	NAPTR	□
Transport	None	Next Hop Priority	☑
Next Hop In-Dialog	□	Ignore Route Header	□
ENUM	□	ENUM Suffix	

Priority / Weight	Server Configuration	Next Hop Address	Transport	
1	SP4	192.168.64.176:5060 (UDP)	None	Delete

Figure 39 - Routing to Windstream

6.2.7. Configure Topology Hiding – Avaya IP Office

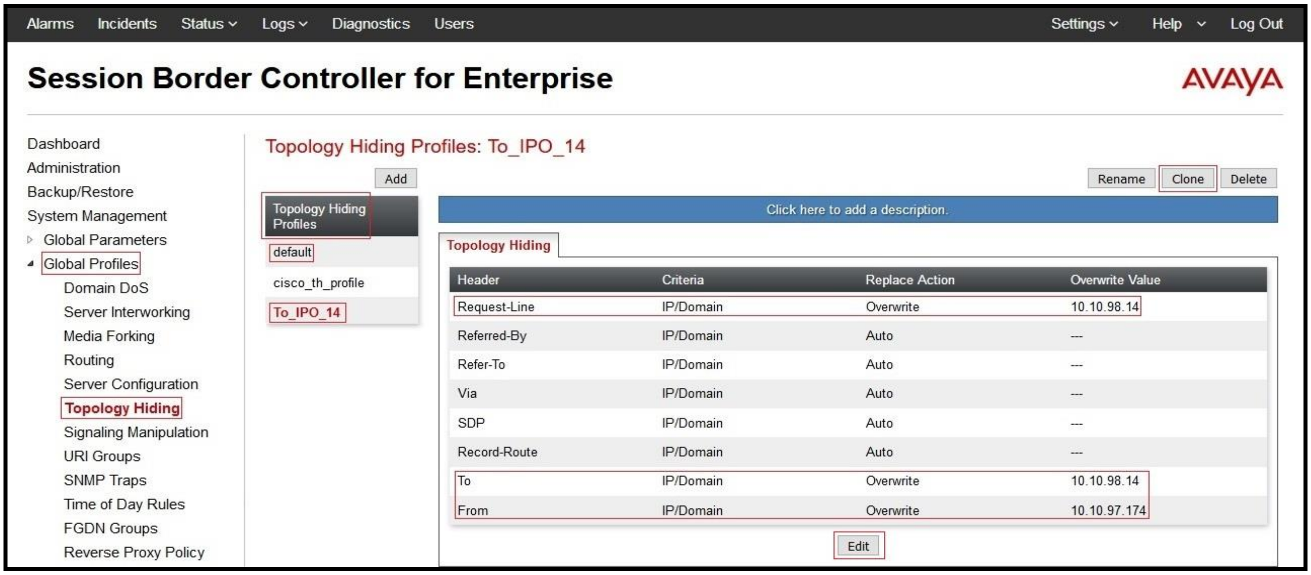
The **Topology Hiding** screen allows an administrator to manage how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the integrity of the network. It hides the topology of the enterprise network from external networks.

From the menu on the left-hand side, select **Global Profiles → Topology Hiding**

- Select **default** in **Topology Hiding Profiles**
- Click **Clone**
- Enter **Clone Name**: **To_IPO_14** and click **Finish** (not shown)
- Select **To_IPO_14** in **Topology Hiding Profiles** and click **Edit** button to modify as below:
  For the Header **Request-Line**,
  - In the **Criteria** column, select **IP/Domain**
  - In the **Replace Action** column, select Overwrite
  - In the **Overwrite Value** column, enter **10.10.98.14** (Avaya IP Office LAN2 port IP address)

  For the Header **To**,
  - In the **Criteria** column, select **IP/Domain**
  - In the **Replace Action** column, select **Overwrite**
  - In the **Overwrite Value** column, enter **10.10.98.14** (Avaya IP Office LAN2 port IP address)

  For the Header **From**,
  - In the **Criteria** column, select **IP/Domain**
  - In the **Replace Action** column, select **Overwrite**
  - In the Overwrite Value column, enter **10.10.97.174** (Avaya SBCE internal IP address)
- Click **Finish** (not shown)



Topology Hiding Profiles: To_IPO_14

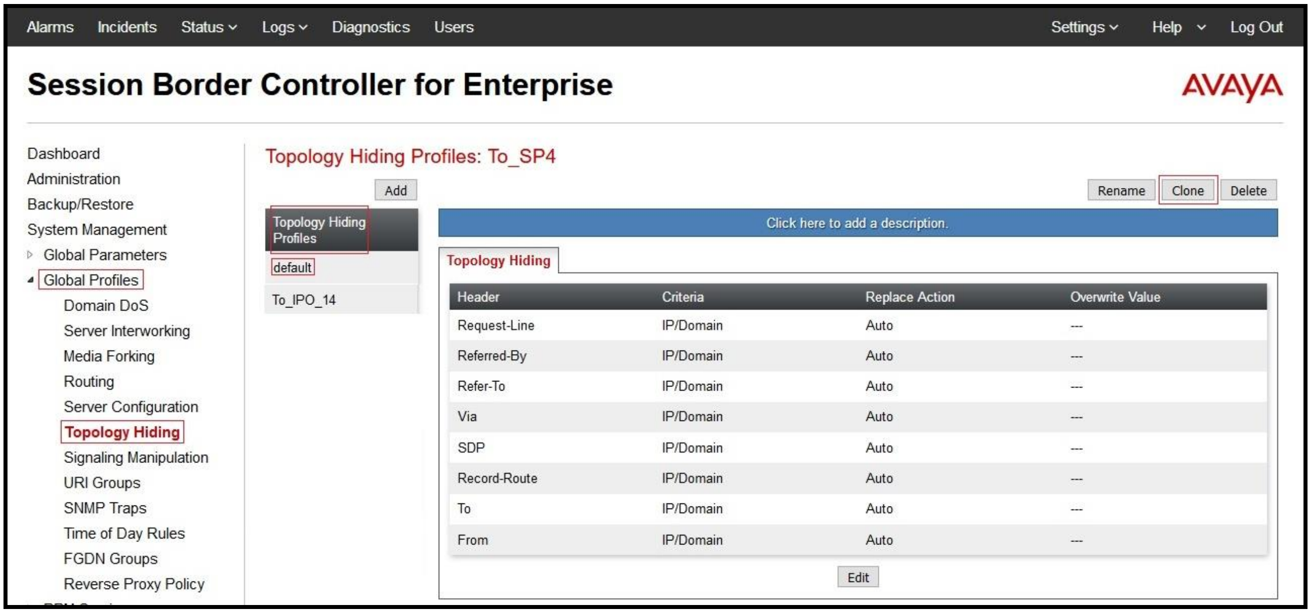
Header	Criteria	Replace Action	Overwrite Value
Request-Line	IP/Domain	Overwrite	10.10.98.14
Referred-By	IP/Domain	Auto	---
Refer-To	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
SDP	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
To	IP/Domain	Overwrite	10.10.98.14
From	IP/Domain	Overwrite	10.10.97.174

Figure 40 - Topology Hiding Avaya IP Office

6.2.8. Configure Topology Hiding – Windstream

From the menu on the left-hand side, select **Global Profiles → Topology Hiding**

- Select **default** in **Topology Hiding Profiles**
- Click **Clone**
- Enter **Clone Name**: **To_SP4** and click **Finish** (not shown)



Topology Hiding Profiles: To_SP4

Header	Criteria	Replace Action	Overwrite Value
Request-Line	IP/Domain	Auto	---
Referred-By	IP/Domain	Auto	---
Refer-To	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
SDP	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
To	IP/Domain	Auto	---
From	IP/Domain	Auto	---

Figure 41 - Topology Hiding Windstream

6.3. Domain Policies

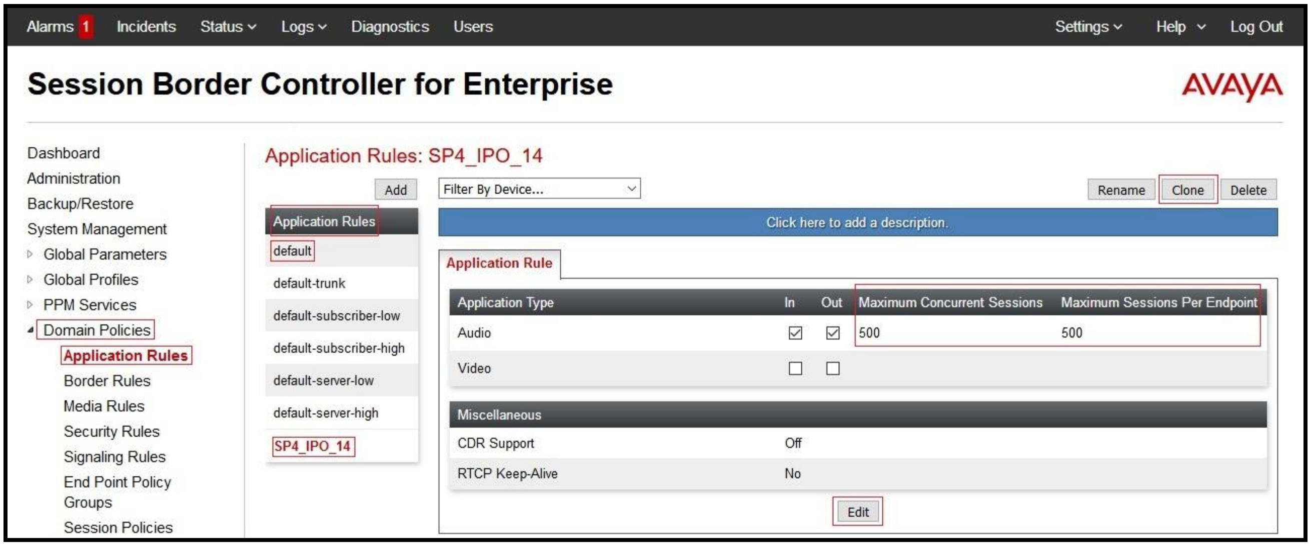
The Domain Policies feature allows administrator to configure, apply, and manage various rule sets (policies) to control unified communications based upon various criteria of communication sessions originating from or terminating in the enterprise. These criteria can be used to trigger different policies which will apply on call flows, change the behavior of the call, and make sure the call does not violate any of the policies. There are default policies available to use, or an administrator can create a custom domain policy.

6.3.1. Create Application Rules

Application Rules allow one to define which types of Avaya applications will be passed. The Avaya SBCE security device will protect: voice, video, and/or Instant Messaging (IM). In addition, one can determine the maximum number of concurrent voice and video sessions so that the network will process to prevent resource exhaustion. For the compliance test, the **SP4_IPO_14** application rule (shown below) was used for the End Point Policy Group defined in **Section 6.3.3**.

From the menu on the left-hand side, select **Domain Policies → Application Rules**

- Select the **default** rule and click on **Clone** button
- Enter **Clone Name**: **SP4_IPO_14** and click **Finish** button (not shown)
- Select the **SP4_IPO_14** rule from the list of **Application Rules** and click on **Edit** button
- Set **Maximum Concurrent Sessions** to **500** and **Maximum Sessions Per Endpoint** to **500**
- Click **Finish** button (not shown) to save the changes



Application Rules: SP4_IPO_14

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	☑	☑	500	500
Video	□	□		

Miscellaneous	
CDR Support	Off
RTCP Keep-Alive	No

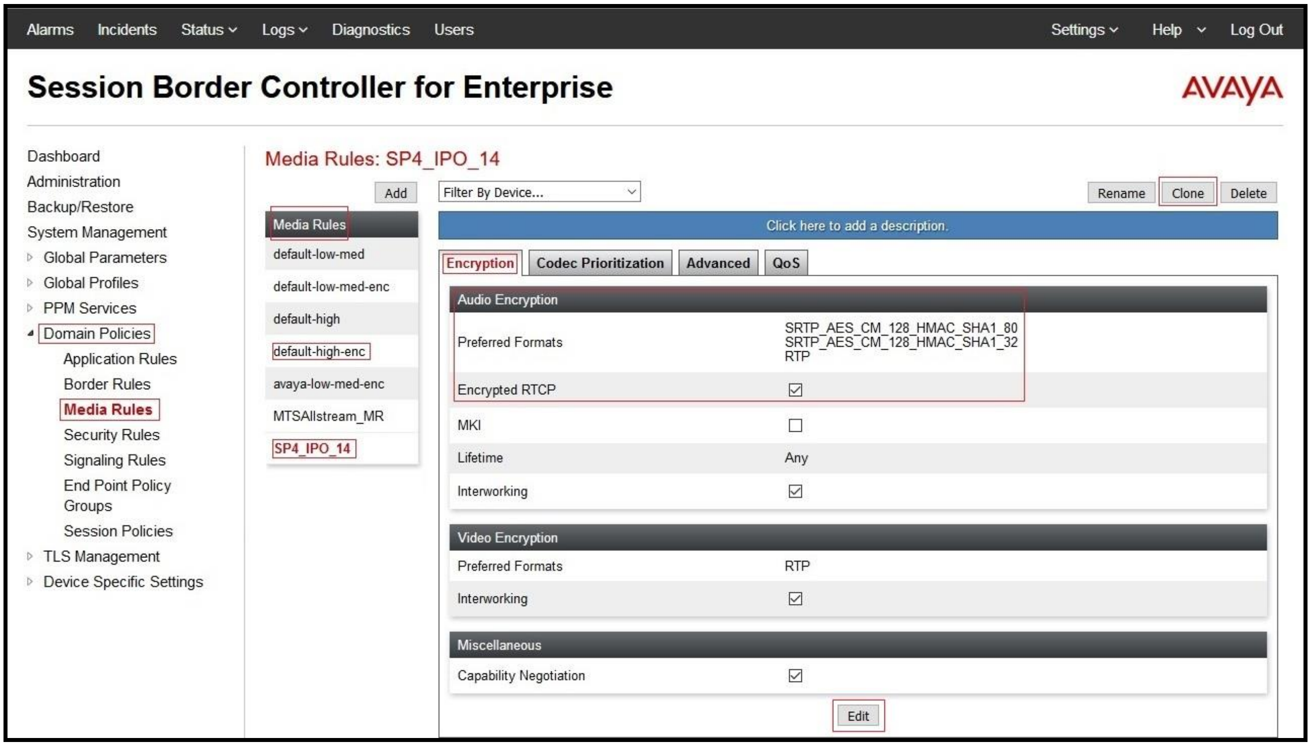
Figure 42 – Application Rule

6.3.2. Create Media Rules

Media Rules allow one to define SRTP, RTP media packet parameters such as prioritizing encryption techniques and packet encryption techniques. Together these media-related parameters define a strict profile that is associated with other SIP-specific policies to determine how media packets matching these criteria will be handled by the Avaya SBCE. For the compliance test, the predefined **default-high-enc** media rule (shown below) was used to clone for media rule.

From the menu on the left-hand side, select **Domain Policies → Media Rules**

- Select the **default-high-enc** rule, click **Clone**. Enter **Clone Name**: **SP4_IPO_14**. Click **Finish** (not shown)
- Select **SP4_IPO_14** under the list of **Media Rules** and click on **Edit** button to modify. The **Encryption** tab indicates that **SRTP_AES_CM_128_HMAC_SHA1_80**, **SRTP_AES_CM_128_HMAC_SHA1_32**, and **RTP** audio encryption were used. Make sure to check **Encrypted RTCP** and leave Lifetime as blank to match any values.



Media Rules: SP4_IPO_14

Audio Encryption

Preferred Formats	SRTP_AES_CM_128_HMAC_SHA1_80 SRTP_AES_CM_128_HMAC_SHA1_32 RTP
Encrypted RTCP	☑
MKI	□
Lifetime	Any
Interworking	☑

Video Encryption

Preferred Formats	RTP
Interworking	☑

Miscellaneous

Capability Negotiation	☑

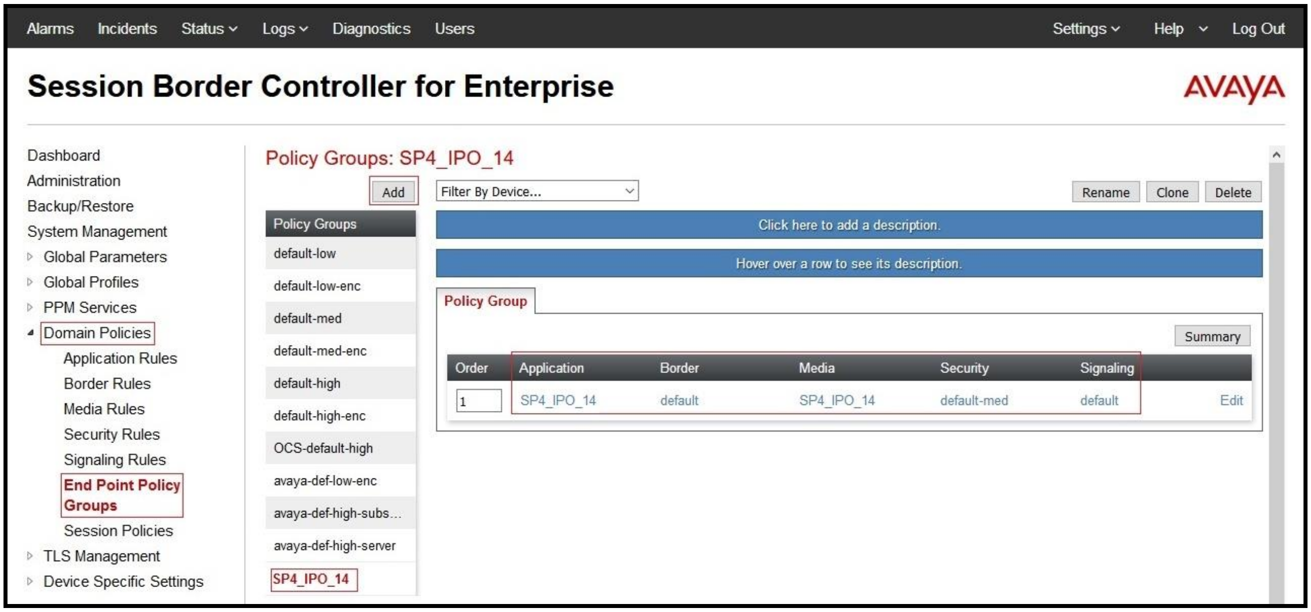
Figure 43 – Media Rule - Encryption

6.3.3. Create Endpoint Policy Groups

The End-Point Policy Group feature allows one to create Policy Sets and Policy Groups. A Policy Set is an association of individual, SIP signaling-specific security policies (rule sets): application, border, media, security, and signaling, each of which was created using the procedures contained in the previous sections. A Policy Group is comprised of one or more Policy Sets. The purpose of Policy Sets and Policy Groups is to increasingly aggregate and simplify the application of Avaya SBCE security features to very specific types of SIP signaling messages traversing through the enterprise.

From the menu on the left-hand side, select **Domain Policies → End Point Policy Groups**

- Select **Add**
- Enter **Group Name**: **SP4_IPO_14**
  - **Application Rule**: **SP4_IPO_14** (See **Section 6.3.1**)
  - **Border Rule**: **default**
  - **Media Rule**: **SP4_IPO_14** (See **Section 6.3.2**)
  - **Security Rule**: **default-med**
  - **Signaling Rule**: **default**
- Select **Finish** (not shown)



Policy Groups: SP4_IPO_14

Order	Application	Border	Media	Security	Signaling	
1	SP4_IPO_14	default	SP4_IPO_14	default-med	default	Edit

Figure 44 – End Point Policy

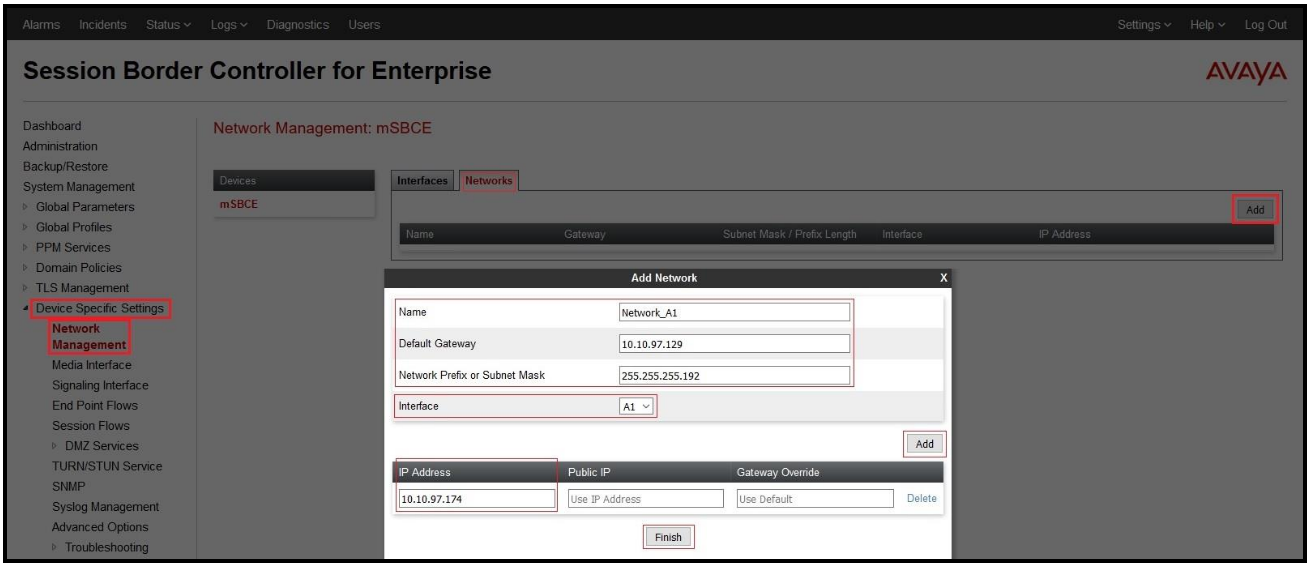
6.4. Device Specific Settings

The Device Specific Settings feature for SIP allows one to view aggregate system information, and manage various device-specific parameters which determine how a particular device will function when deployed in the network. Specifically, one has the ability to define and administer various device-specific protection features such as Message Sequence Analysis (MSA) functionality, end-point and session call flows and Network Management.

6.4.1. Manage Network Settings

From the menu on the left-hand side, select **Device Specific Settings → Network Management**

- Select **Networks** tab and click the **Add** button to add a network for the inside interface as follows:
  - **Name**: **Network_A1**
  - **Default Gateway**: **10.10.97.129**
  - **Network Prefix or Subnet Mask**: **255.255.255.192**
  - **Interface**: **A1** (This is the Avaya SBCE internal interface)
  - Click the **Add** button to add the **IP Address** for inside interface: **10.10.97.174**
  - Click the **Finish** button to save the changes



Session Border Controller for Enterprise

Network Management: mSBCE

Add Network

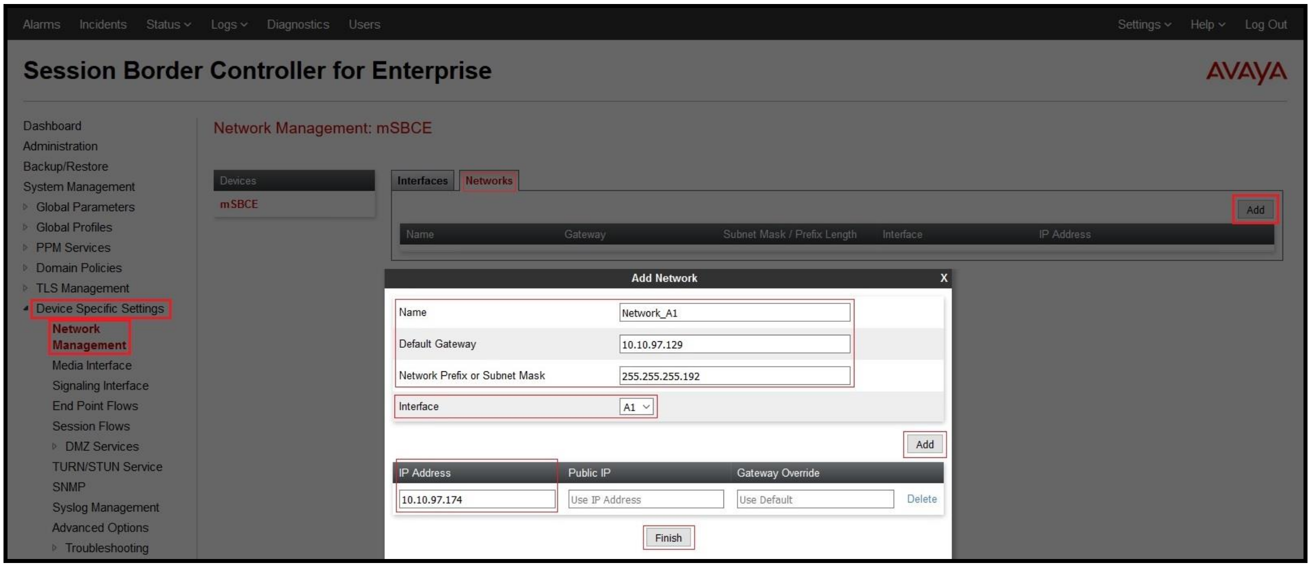
Name	Network_A1
Default Gateway	10.10.97.129
Network Prefix or Subnet Mask	255.255.255.192
Interface	A1

IP Address	Public IP	Gateway Override
10.10.97.174	Use IP Address	Use Default

Figure 45 - Network Management – Inside Interface

From the menu on the left-hand side, select **Device Specific Settings → Network Management**

- Select **Networks** tab and click the **Add** button to add a network for the inside interface as follows:
  - **Name**: **Network_A1**
  - **Default Gateway**: **10.10.97.129**
  - **Network Prefix or Subnet Mask**: **255.255.255.192**
  - **Interface**: **A1** (This is the Avaya SBCE internal interface)
  - Click the **Add** button to add the **IP Address** for inside interface: **10.10.97.174**
  - Click the **Finish** button to save the changes



Name	Network_A1
Default Gateway	10.10.97.129
Network Prefix or Subnet Mask	255.255.255.192
Interface	A1

Add

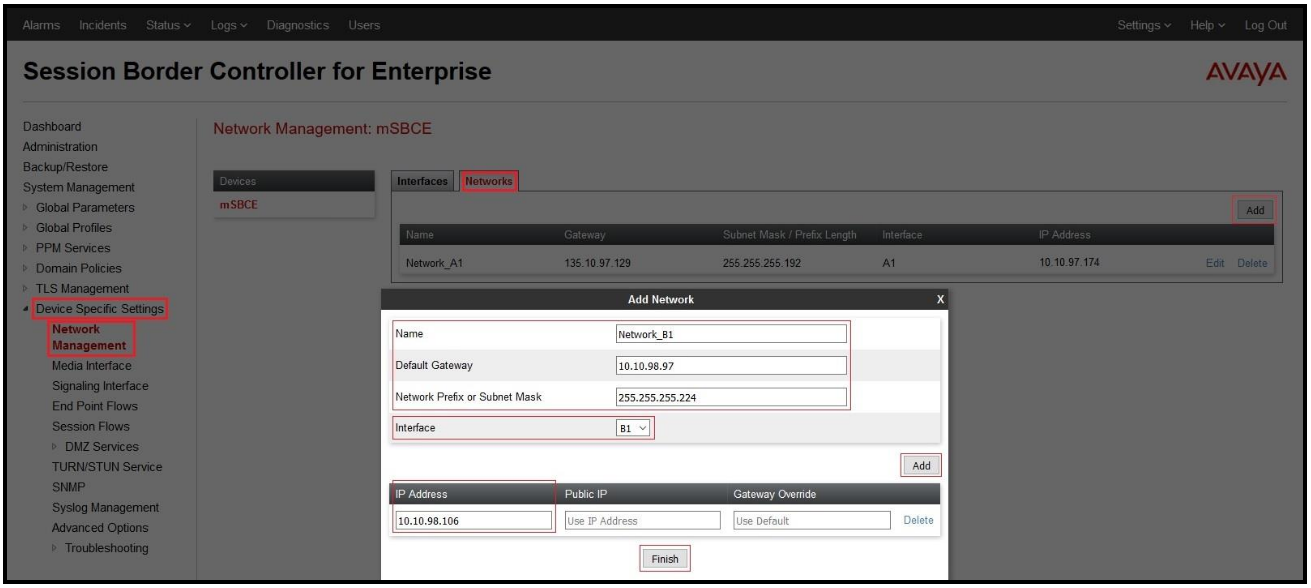
IP Address	Public IP	Gateway Override	
10.10.97.174	Use IP Address	Use Default	Delete

Finish

Figure 46 - Network Management – Inside Interface

From the menu on the left-hand side, select **Device Specific Settings → Network Management**

- Select **Networks** tab and click the **Add** button to add a network for the external interface as follows:
  - **Name**: **Network_B1**
  - **Default Gateway**: **10.10.98.97**
  - **Network Prefix or Subnet Mask**: **255.255.255.224**
  - **Interface**: **B1** (This is the Avaya SBCE outside interface)
  - Click the **Add** button to add the **IP Address** for external interface: **10.10.98.106**
  - Click the **Finish** button to save the changes



Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address		
Network_A1	135.10.97.129	255.255.255.192	A1	10.10.97.174	Edit	Delete

Add Network

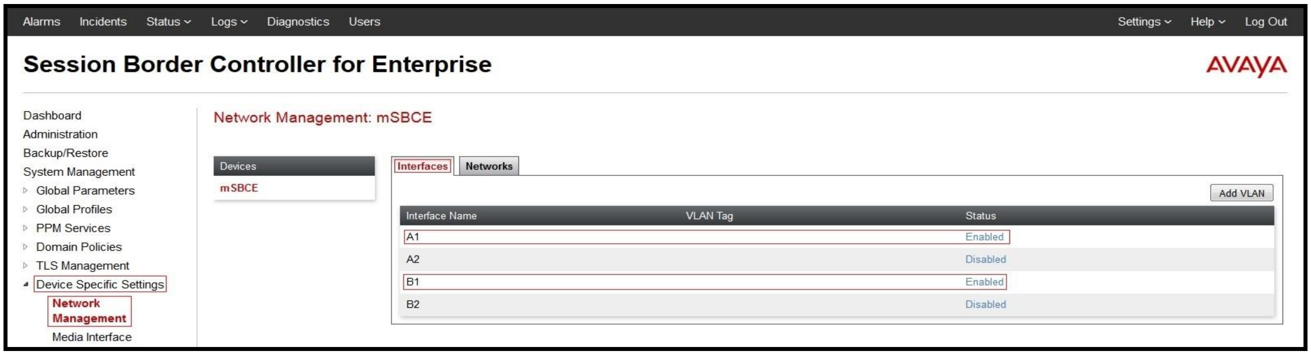
Name	Network_B1
Default Gateway	10.10.98.97
Network Prefix or Subnet Mask	255.255.255.224
Interface	B1

IP Address	Public IP	Gateway Override	
10.10.98.106	Use IP Address	Use Default	Delete

Figure 47 - Network Management – External Interface

From the menu on the left-hand side, select **Device Specific Settings → Network Management**

- Select the **Interfaces** tab
- Click on the **Status** of the physical interfaces being used and change them to **Enabled** state



Interface Name	VLAN Tag	Status
A1		Enabled
A2		Disabled
B1		Enabled
B2		Disabled

Figure 48 - Network Management – Interface Status

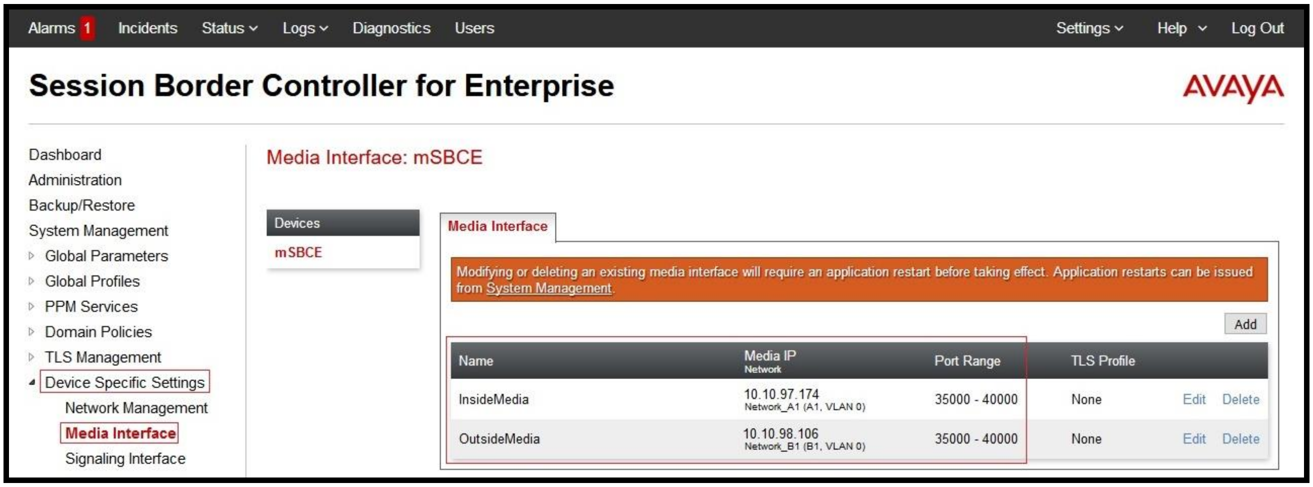
6.4.2. Create Media Interfaces

Media Interfaces define the type of media on the ports. The default media port range on the Avaya SBCE can be used for both inside and outside ports.

From the menu on the left-hand side, **Device Specific Settings → Media Interface**

- Select the **Add** button and enter the following in the configuration window (not shown):
    - **Name**: **InsideMedia**
    - **IP Address**: Select **Network_A1 (A1,VLAN0)** and **10.10.97.174** (Avaya SBCE internal IP address toward Avaya IP Office)
    - **Port Range**: **35000 – 40000**
    - Click **Finish** (not shown)
- Select the **Add** button and enter the following in the configuration window (not shown):
    - **Name**: **OutsideMedia**
    - **IP Address**: Select **Network_B1 (B1,VLAN0)** and **10.10.98.106** (Avaya SBCE external IP address toward Windstream)
    - **Port Range**: **35000 – 40000**
    - Click **Finish** (not shown)

The screen below shows the configured media interfaces:



Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management.

Name	Media IP Network	Port Range	TLS Profile		
InsideMedia	10.10.97.174 Network_A1 (A1, VLAN 0)	35000 - 40000	None	Edit	Delete
OutsideMedia	10.10.98.106 Network_B1 (B1, VLAN 0)	35000 - 40000	None	Edit	Delete

Figure 49 - Media Interface

6.4.3. Create Signaling Interfaces

Signaling Interfaces define the type of signaling on the ports.

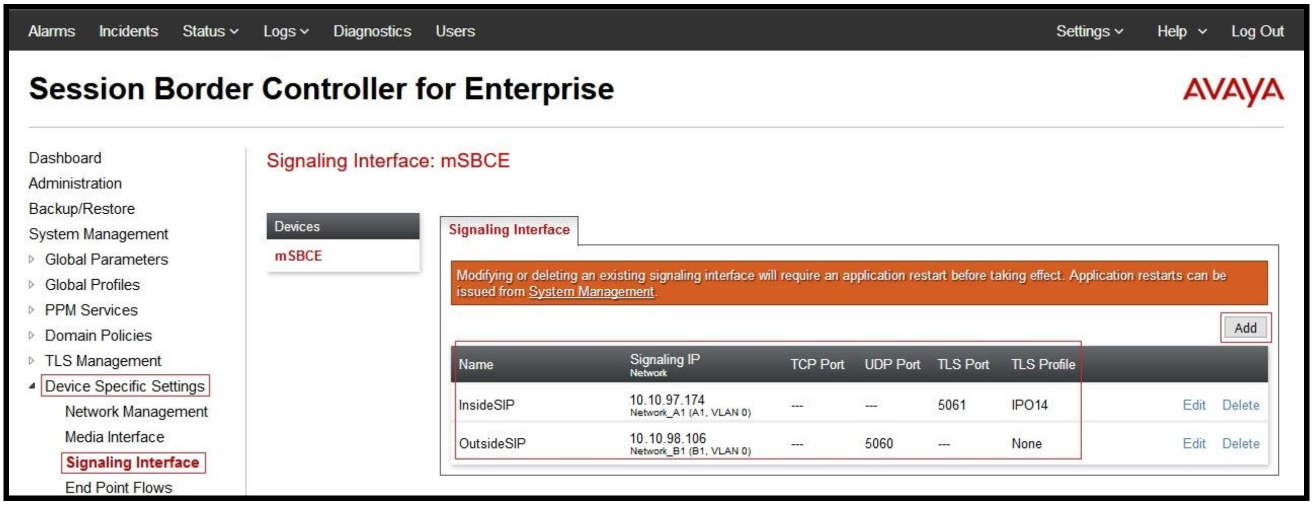
From the menu on the left-hand side, select **Device Specific Settings → Signaling Interface**

- Select the **Add** button and enter the following in the configuration window (not shown):
  - **Name**: **InsideSIP**
  - **IP Address**: Select **Network_A1 (A1,VLAN0)** and **10.10.97.174** (Avaya SBCE internal IP address toward Avaya IP Office)
  - **TLS Port**: **5061**
  - **TLS Profile: IPO14**. Note: During the compliance test in the lab environment, demo certificates are used and are not recommended for production use. Consult the appropriate Avaya product documentation for further information regarding security certificate and encryption capabilities supported by Avaya product
  - Click **Finish** (not shown)

From the menu on the left-hand side, select **Device Specific Settings → Signaling Interface**

- Select the **Add** button and enter the following in the configuration window (not shown):
  - **Name**: **OutsideSIP**
  - **IP Address**: Select **Network_B1 (B1,VLAN0)** and **10.10.98.106** (Avaya SBCE external IP address toward Windstream)
  - **UDP Port**: **5060**
  - Click **Finish** (not shown)

The screen below shows the configured signaling interfaces:



Modifying or deleting an existing signaling interface will require an application restart before taking effect. Application restarts can be issued from System Management.

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile		
InsideSIP	10.10.97.174 Network_A1 (A1, VLAN 0)	---	---	5061	IPO14	Edit	Delete
OutsideSIP	10.10.98.106 Network_B1 (B1, VLAN 0)	---	5060	---	None	Edit	Delete

Figure 50 - Signaling Interface

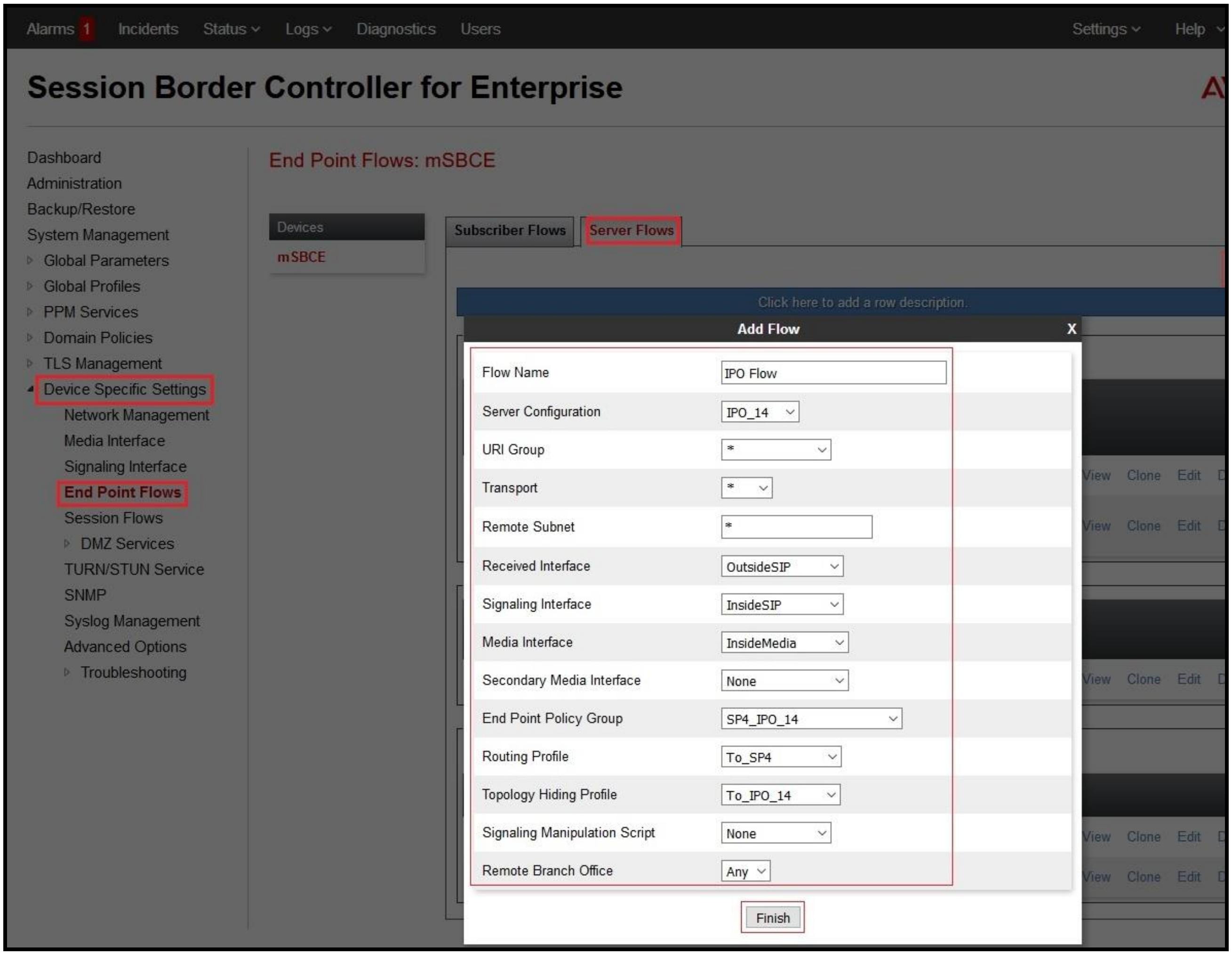
6.4.4. Configuration Server Flows

Server Flows allow an administrator to categorize signaling and apply various policies.

6.4.4.1 Create End Point Flows – Avaya IP Office

From the menu on the left-hand side, select **Device Specific Settings → End Point Flows**

- Select the **Server Flows** tab
- Select **Add**, enter the followings:
  - **Flow Name**: **IPO Flow**
  - **Server Configuration**: **IPO_14** (see **Section 6.2.3**)
  - **URI Group**: *
  - **Transport**: *
  - **Remote Subnet**: *
  - **Received Interface**: **OutsideSIP** (see **Section 6.4.3**)
  - **Signaling Interface**: **InsideSIP** (see **Section 6.4.3**)
  - **Media Interface**: **InsideMedia** (see **Section 6.4.2**)
  - **Secondary Media Interface**: **None**
  - **End Point Policy Group**: **SP4_IPO_14** (see **Section 6.3.3**)
  - **Routing Profile**: **To_SP4** (see **Section 6.2.6**)
  - **Topology Hiding Profile**: **To_IPO_14** (see **Section 6.2.7**)
  - Leave other options as default
  - Click **Finish**



Flow Name	IPO Flow
Server Configuration	IPO_14
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	OutsideSIP
Signaling Interface	InsideSIP
Media Interface	InsideMedia
Secondary Media Interface	None
End Point Policy Group	SP4_IPO_14
Routing Profile	To_SP4
Topology Hiding Profile	To_IPO_14
Signaling Manipulation Script	None
Remote Branch Office	Any

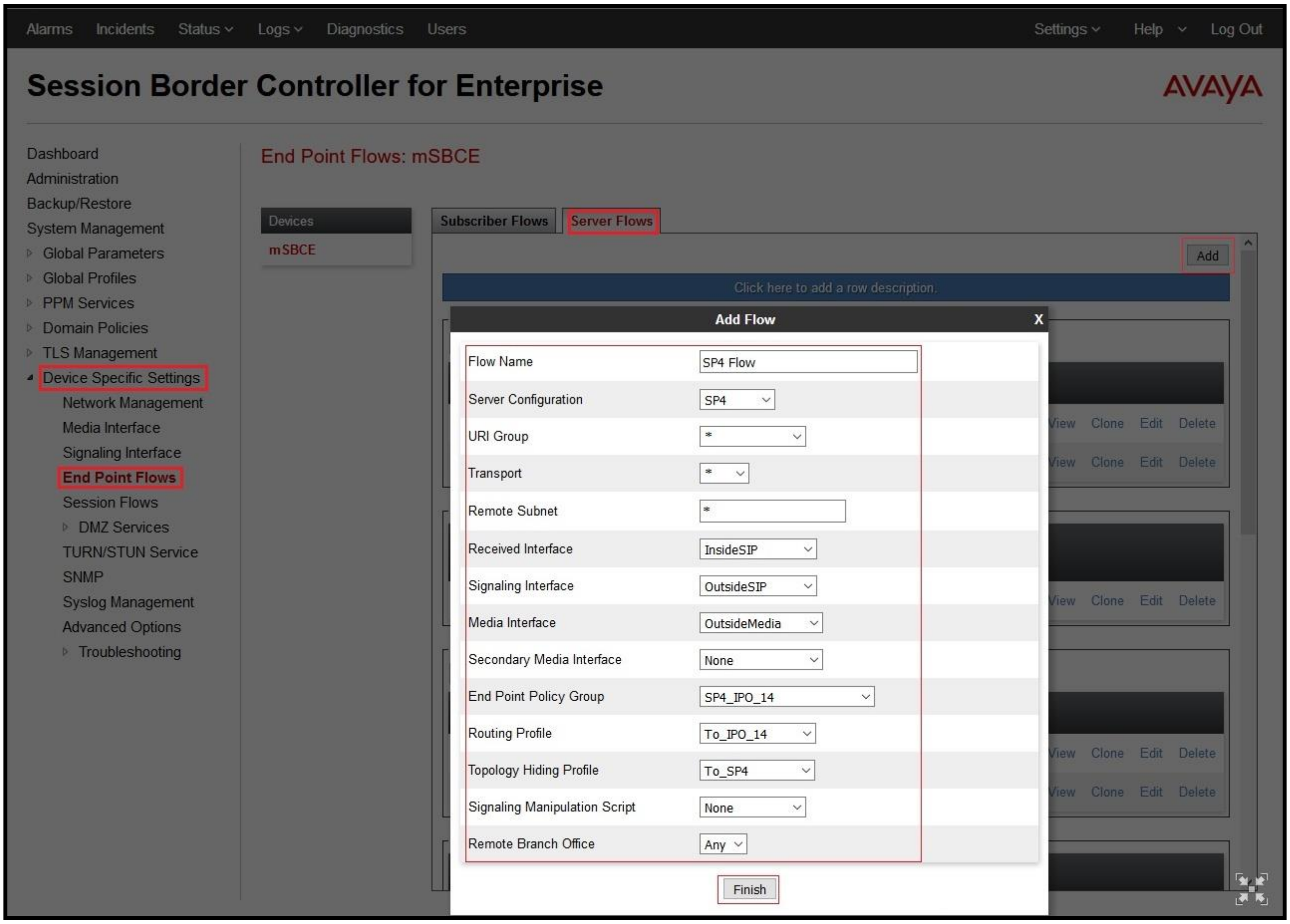
Figure 51 - End Point Flow to Windstream

6.4.4.2 Create End Point Flows – Windstream

From the menu on the left-hand side, select **Device Specific Settings → End Point Flows**

- Select the **Server Flows** tab
- Select **Add**, enter the followings:
  - **Flow Name**: **SP4 Flow**
  - **Server Configuration**: **SP4** (see **Section 6.2.4**)
  - **URI Group**: *****
  - **Transport**: *****
  - **Remote Subnet**: *****
  - **Received Interface**: **InsideSIP** (see **Section 6.4.3**)
  - **Signaling Interface**: **OutsideSIP** (see **Section 6.4.3**)
  - **Media Interface**: **OutsideMedia** (see **Section 6.4.2**)
  - **Secondary Media Interface**: **None**
  - **End Point Policy Group**: **SP4_IPO_14** (see **Section 6.3.3**)
  - **Routing Profile**: **To_IPO_14** (see **Section 6.2.5**)

- **Topology Hiding Profile**: **To_SP4** (see **Section 6.2.8**)
- Leave other options as default
- Click **Finish**



Flow Name	SP4 Flow
Server Configuration	SP4
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	InsideSIP
Signaling Interface	OutsideSIP
Media Interface	OutsideMedia
Secondary Media Interface	None
End Point Policy Group	SP4_IPO_14
Routing Profile	To_IPO_14
Topology Hiding Profile	To_SP4
Signaling Manipulation Script	None
Remote Branch Office	Any

Figure 52 - End Point Flow from Windstream

7. Windstream SIP Trunk Configuration

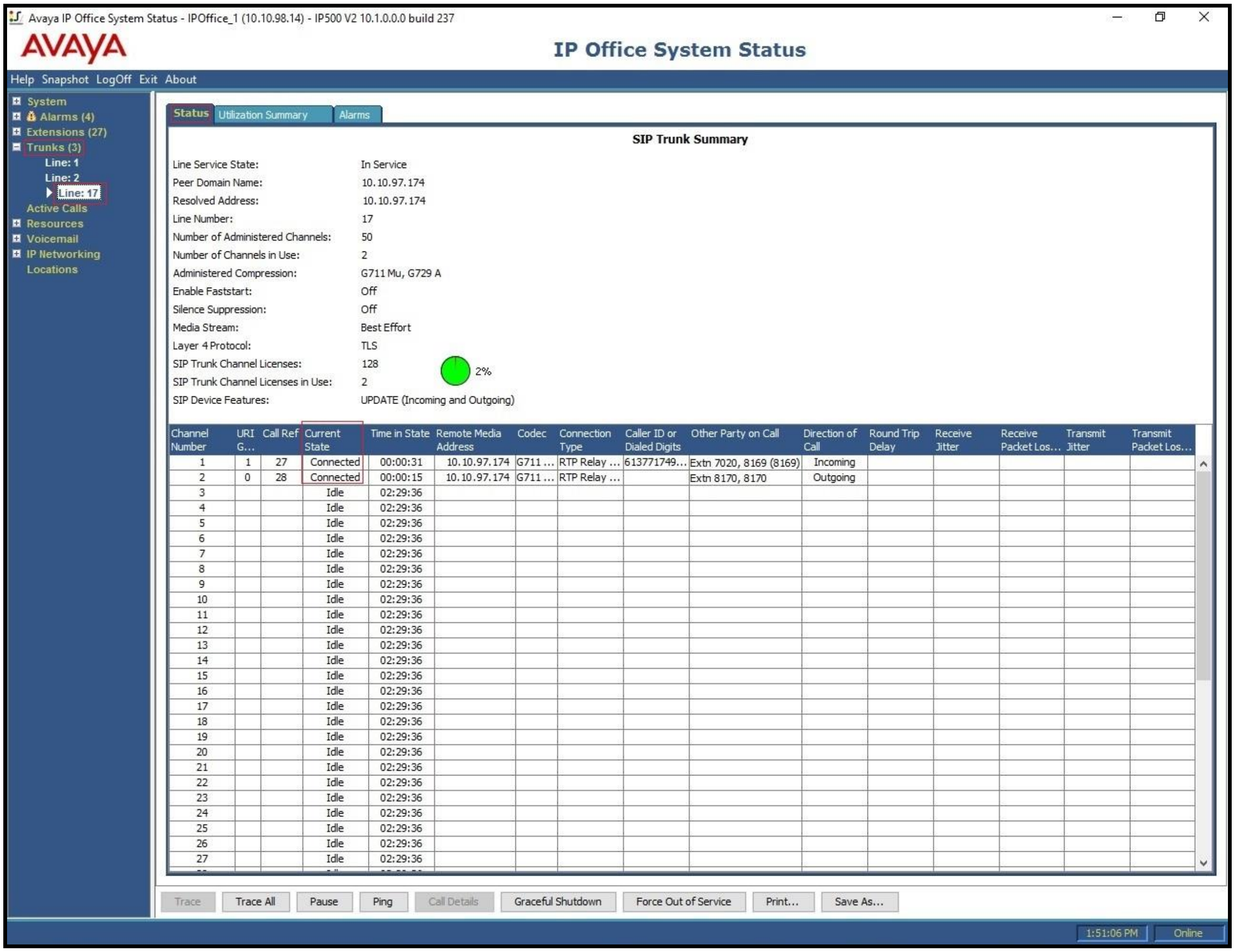
Windstream is responsible for the configuration of Windstream SIP Trunk Service. The customer must provide the IP address used to reach the Avaya SBCE at the enterprise. Windstream will provide the customer necessary information to configure the SIP connection between Avaya SBCE and Windstream. The provided information from Windstream includes:

- IP address and port number used for signaling or media servers through any security devices
- DID numbers
- Windstream SIP Trunk Specification (if applicable)

8. Verification Steps

The following steps may be used to verify the configuration:

- Use the Avaya IP Office System Status application to verify the state of the SIP connection. Launch the application from **Start → Programs → IP Office → System Status** on the PC where Avaya IP Office Manager was installed. Select the SIP Line of interest from the left pane. On the **Status** tab in the right pane, verify that the **Current State** for each channel. (The below screen shot showed 2 active calls at the time.)



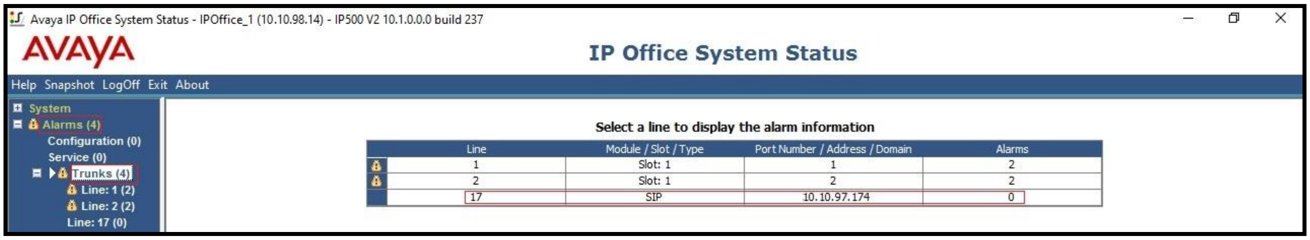
SIP Trunk Summary

Line Service State: In Service
Peer Domain Name: 10.10.97.174
Resolved Address: 10.10.97.174
Line Number: 17
Number of Administered Channels: 50
Number of Channels in Use: 2
Administered Compression: G711 Mu, G729 A
Enable Faststart: Off
Silence Suppression: Off
Media Stream: Best Effort
Layer 4 Protocol: TLS
SIP Trunk Channel Licenses: 128
SIP Trunk Channel Licenses in Use: 2
SIP Device Features: UPDATE (Incoming and Outgoing)

Channel Number	URI G…	Call Ref	Current State	Time in State	Remote Media Address	Codec	Connection Type	Caller ID or Dialed Digits	Other Party on Call	Direction of Call	Round Trip Delay	Receive Jitter	Receive Packet Los…	Transmit Jitter	Transmit Packet Los…
1	1	27	Connected	00:00:31	10.10.97.174	G711 …	RTP Relay …	613771749…	Extn 7020, 8169 (8169)	Incoming					
2	0	28	Connected	00:00:15	10.10.97.174	G711 …	RTP Relay …		Extn 8170, 8170	Outgoing					
3			Idle	02:29:36											
4			Idle	02:29:36											
5			Idle	02:29:36											
6			Idle	02:29:36											
7			Idle	02:29:36											
8			Idle	02:29:36											
9			Idle	02:29:36											
10			Idle	02:29:36											
11			Idle	02:29:36											
12			Idle	02:29:36											
13			Idle	02:29:36											
14			Idle	02:29:36											
15			Idle	02:29:36											
16			Idle	02:29:36											
17			Idle	02:29:36											
18			Idle	02:29:36											
19			Idle	02:29:36											
20			Idle	02:29:36											
21			Idle	02:29:36											
22			Idle	02:29:36											
23			Idle	02:29:36											
24			Idle	02:29:36											
25			Idle	02:29:36											
26			Idle	02:29:36											
27			Idle	02:29:36											

Figure 53 – SIP Trunk status

- Use the Avaya IP Office System Status application to verify that no alarms are active on the SIP line. Launch the application from **Start → Programs → IP Office → System Status** on the PC where Avaya IP Office Manager was installed. Select **Alarm → Trunks** to verify that no alarms are active on the SIP line.


Avaya IP Office System Status - IPOffice_1 (10.10.98.14) - IP500 V2 10.1.0.0.0 build 237
AVAYA
IP Office System Status
Help Snapshot LogOff Exit About
System
Alarms (4)
Configuration (0)
Service (0)
Trunks (4)
Line: 1 (2)
Line: 2 (2)
Line: 17 (0)

Select a line to display the alarm information

	Line	Module / Slot / Type	Port Number / Address / Domain	Alarms
⚠	1	Slot: 1	1	2
⚠	2	Slot: 1	2	2
	17	SIP	10.10.97.174	0

Figure 54 – SIP Trunk alarm

- Verify that a phone connected to the PSTN can successfully place a call to Avaya IP Office with two-way audio.
- Verify that a phone connected to Avaya IP Office can successfully place a call to the PSTN with two-way audio.
- Capture SIP call traces on Avaya SBCE by executing command via the Command Line Interface (CLI): Login Avaya SBCE with root user and enter the command: #traceSBC. The tool updates the database directly based on which trace mode is selected.

9. Conclusion

Windstream passed compliance testing with the limitation listed in **Section □**. These Application Notes describe the procedures required to configure SIP trunk connectivity between Avaya IP Office 10.1 and the Avaya SBCE 7.2 to support Windstream SIP Trunking service, as shown in **Figure 1**.

10. Additional References

[1] Administering Avaya IP Office Platform with Manager, Release 10.1, 15-601011, Issue 14, July 2017.

[2] Deploying Avaya IP Office^{TM} Platform IP500V2, Release 10.1, 15-601042, Issue 32d, May 2017.

[3] Avaya IP Office™ Platform Release 10.1 - Release Notes / Technical Bulletin General Availability

[4] Avaya Session Border Controller for Enterprise 7.2 Release Notes, Issue 1, June 2017

Product documentation for Avaya products may be found at: http://support.avaya.com. Additional IP Office documentation can be found at: http://marketingtools.avaya.com/knowledgebase/ipoffice/general/rss2html.php?XMLFILE=manuals.xml&TEMPLATE=pdf_feed_template.html

Product documentation for Windstream SIP Trunking may be found at: https://www.windstreambusiness.com/solutions/voice-unified-communications/sip-trunking

11. Appendix - Remote Worker Configuration via Avaya SBCE

This section describes the process for connecting remote Avaya SIP endpoints on the public Internet to Avaya IP Office on the private enterprise network via the Avaya SBCE. The provisioning builds on the reference configuration described in previous sections of this document.

For more information, refer to **Section 10**.

Note – This Remote Worker configuration is based on provisioning the Avaya SBCE. It is not to be confused with "native" Avaya IP Office Remote Worker configurations.

In the configuration for the compliance test, Avaya Communicator for Windows (SIP mode) was used as the Remote Worker SIP endpoint.

The reference configuration for the compliance test, including the Remote Worker endpoint, is shown in **Figure 1** in **Section 3**.

11.1. Provisioning Avaya SBCE for Remote Worker

Provisioning of the Avaya SBCE to support Avaya IP Office SIP connection to the service provider is described in **Section 6**. The following sections build on that provisioning.

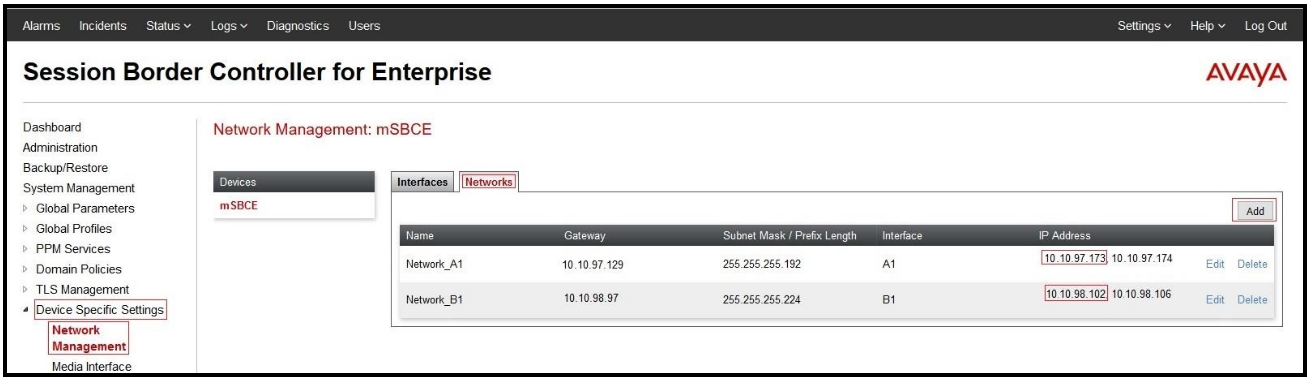
11.1.1. Network Management

This section shows the **Network Management** configuration of the Avaya SBCE to support Remote Worker. For this purpose, the Avaya SBCE is configured with a second outside IP address assigned to physical interface B1, and a second inside IP address assigned to physical interface A1.

The following IP addresses were used on the Avaya SBCE in the configuration used for the compliance test:

- **10.10.97.174** is the inside IP address previously provisioned for SIP Trunking with Avaya IP Office (see **Section 6.4.1**).
- **10.10.97.173** is the new inside IP address for Remote Worker.
- **10.10.98.106** is the outside IP address previously provisioned for SIP Trunking with Windstream (see **Section 6.4.1**).
- **10.10.98.102** is the new outside IP address for Remote Worker.

On the **Networks** tab, select **Add** to create an entry for **10.10.97.173** on interface **A1**, then select **Save** (not shown).
On the **Networks** tab, select **Add** to create an entry for **10.10.98.102** on interface **B1**, then select **Save** (not shown).



Network Management: mSBCE

Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address		
Network_A1	10.10.97.129	255.255.255.192	A1	10.10.97.173, 10.10.97.174	Edit	Delete
Network_B1	10.10.98.97	255.255.255.224	B1	10.10.98.102, 10.10.98.106	Edit	Delete

Figure 55 – Remote Worker Network Management

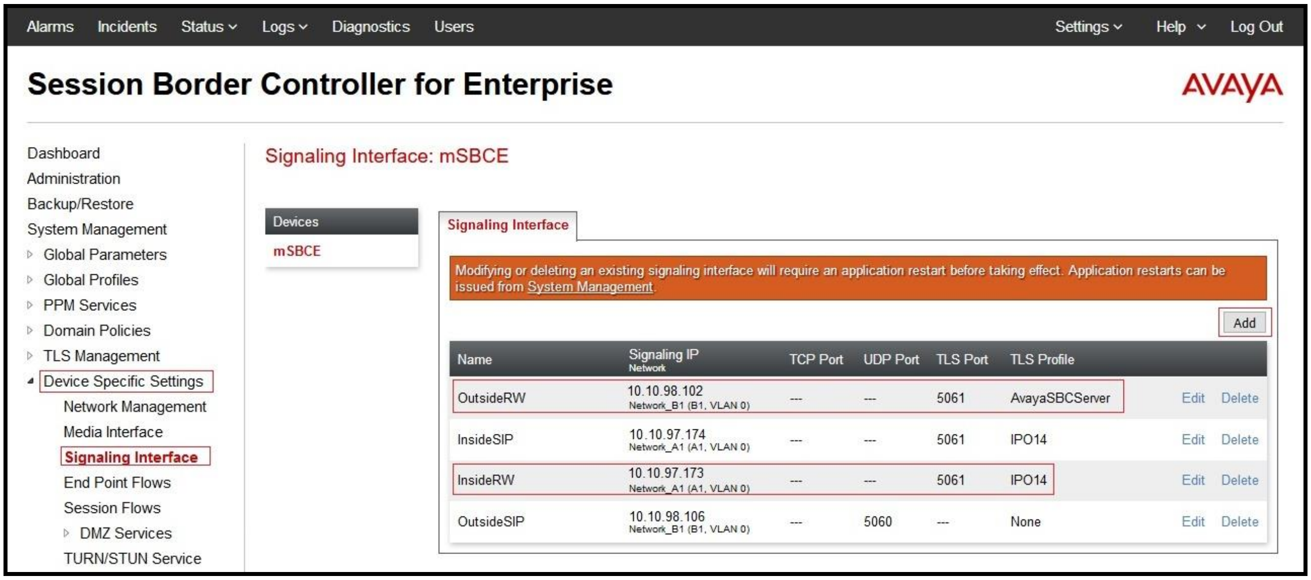
11.1.2. Signaling Interfaces

Two new Signaling interfaces were created for the inside and outside IP interfaces used for Remote Worker SIP traffic. Both interfaces **InsideRW** and **OutsideRW** support **TLS Port 5061**.
From **Device Specific Settings** on the left-hand menu, select **Signaling Interface**. Click on the **Add** button to create Signaling Interface **InsideRW**

- **Signaling IP** = **10.10.97.173**
- **TLS Port** = **5061**
- **TLS Profile** = **IPO14**

From **Device Specific Settings** on the left-hand menu, select **Signaling Interface**. Click on the **Add** button to create Signaling Interface **OutsideRW**

- **Signaling IP** = **10.10.98.102**
- **TLS Port** = **5061**
- **TLS Profile** = **AvayaSBCServer**



Signaling Interface: mSBCE

Modifying or deleting an existing signaling interface will require an application restart before taking effect. Application restarts can be issued from System Management.

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile		
OutsideRW	10.10.98.102 Network_B1 (B1, VLAN 0)	---	---	5061	AvayaSBCServer	Edit	Delete
InsideSIP	10.10.97.174 Network_A1 (A1, VLAN 0)	---	---	5061	IPO14	Edit	Delete
InsideRW	10.10.97.173 Network_A1 (A1, VLAN 0)	---	---	5061	IPO14	Edit	Delete
OutsideSIP	10.10.98.106 Network_B1 (B1, VLAN 0)	---	5060	---	None	Edit	Delete

Figure 56 – Remote Worker Signaling Interface

Signaling Interface **InsideRW** is used in the Remote Worker Server Flow (Refer to **Section 11.1.9.2**). Signaling Interface **OutsideRW** is used in the Remote Worker Subscriber Flow (Refer to **Section 11.1.9.1**), and in the Remote Worker Server Flow (Refer to **Section 11.1.9.2**).

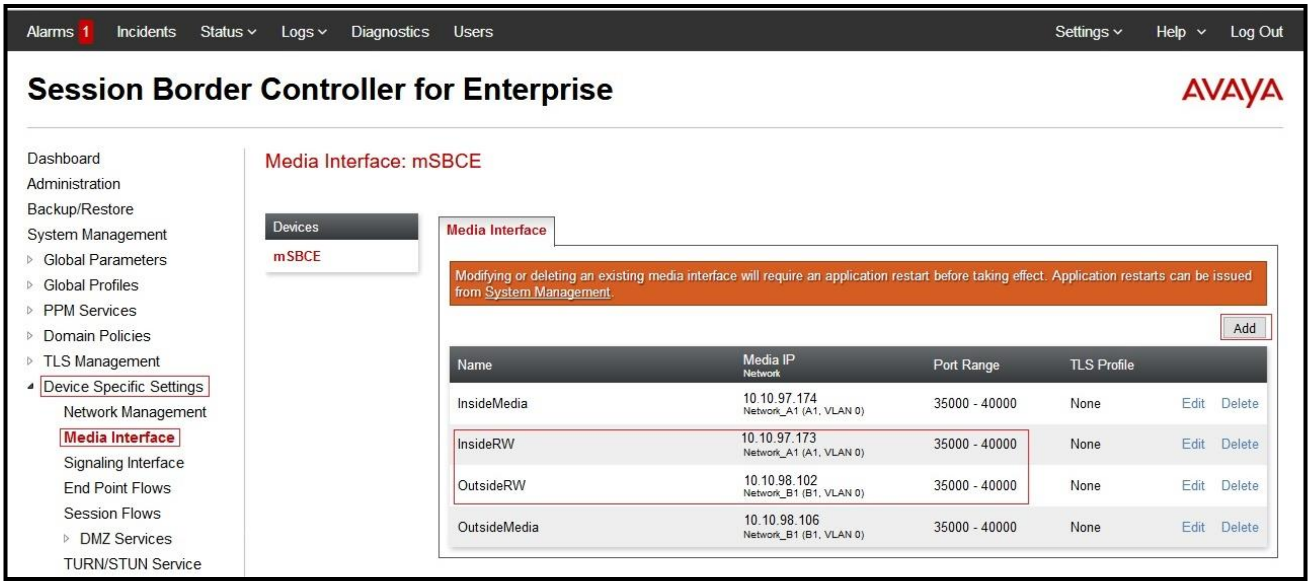
11.1.3. Media Interface

Two new Media interfaces were created for the inside and outside IP interfaces used for Remote Worker SIP traffic.
From **Device Specific Settings** on the left-hand menu, select **Media Interface**. Click on the **Add** button to create Media Interface **InsideRW** using the parameters shown below:

- **Media IP** = **10.10.97.173**
- **Port Range** = **35000 – 40000**

From **Device Specific Settings** on the left-hand menu, select **Media Interface**. Click on the **Add** button to create Media Interface **OutsideRW** using the parameters shown below:

- **Media IP** = **10.10.98.102**
- **Port Range** = **35000 – 40000**



Session Border Controller for Enterprise

Media Interface: mSBCE

Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management.

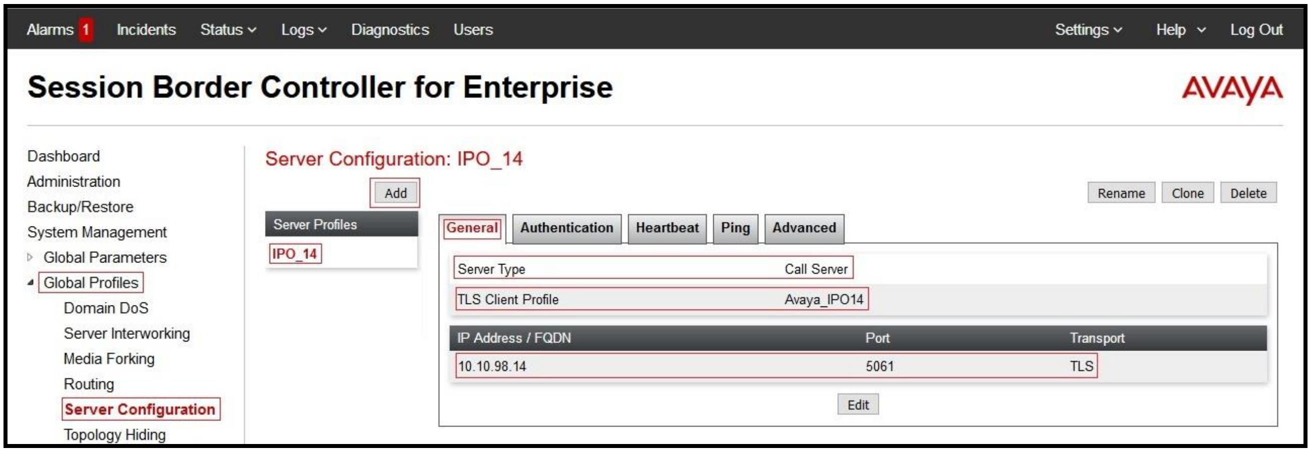
Name	Media IP Network	Port Range	TLS Profile		
InsideMedia	10.10.97.174 Network_A1 (A1, VLAN 0)	35000 - 40000	None	Edit	Delete
InsideRW	10.10.97.173 Network_A1 (A1, VLAN 0)	35000 - 40000	None	Edit	Delete
OutsideRW	10.10.98.102 Network_B1 (B1, VLAN 0)	35000 - 40000	None	Edit	Delete
OutsideMedia	10.10.98.106 Network_B1 (B1, VLAN 0)	35000 - 40000	None	Edit	Delete

Figure 57 – Remote Worker Media Interface

Media Interface **InsideRW** is used in the Remote Worker Server Flow (Refer to **Section 11.1.9.2**). Media Interface **OutsideRW** is used in the Remote Worker Subscriber Flow (Refer to **Section 11.1.9.1**).

11.1.4. Server Profile for Avaya IP Office

The existing **IPO_14** Server Profile (Defined in **Section 6.2.3**) is used for Remote Worker.



Server Configuration: IPO_14

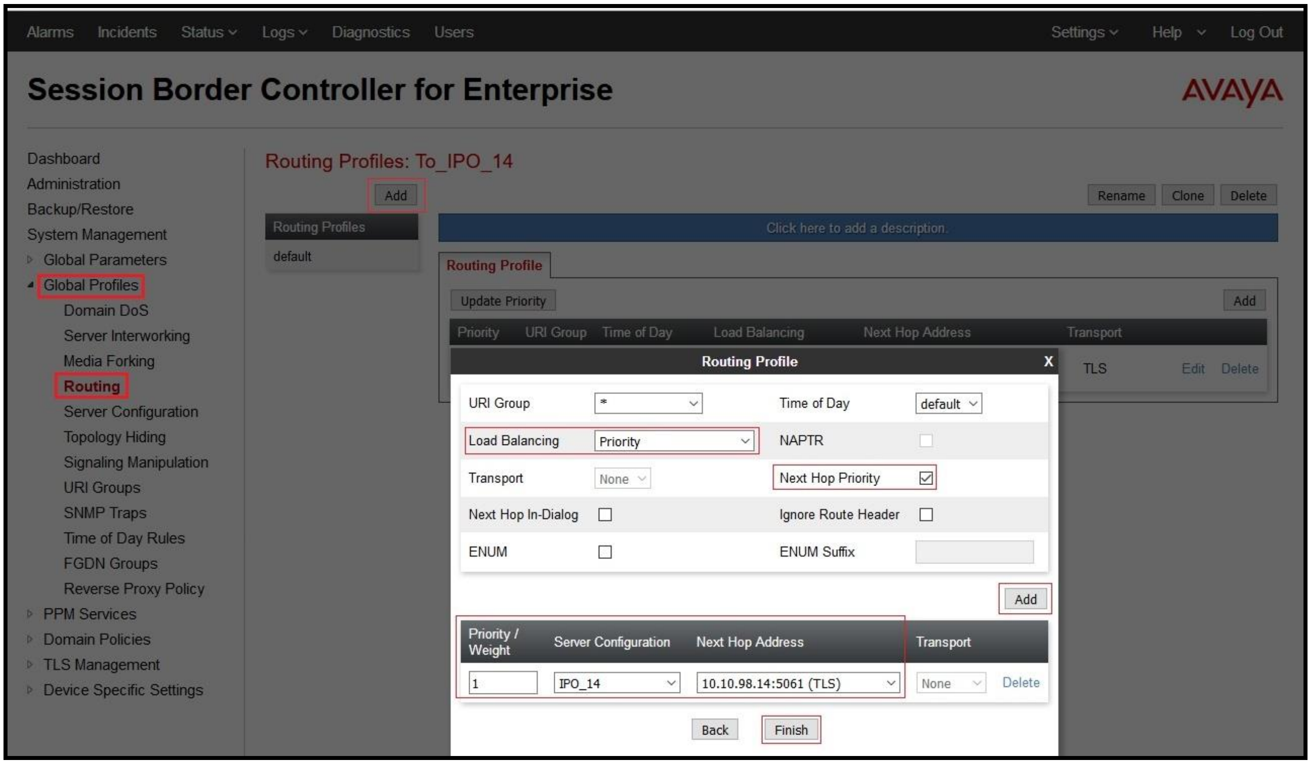
Server Type	Call Server
TLS Client Profile	Avaya_IPO14

IP Address / FQDN	Port	Transport
10.10.98.14	5061	TLS

Figure 58 – Remote Worker Server Configuration

11.1.5. Routing Profiles

Two Routing Profiles are required to support Remote Worker
The existing **To_IPO_14** Routing (see **Section 6.2.5**) is used for Remote Worker.



Routing Profiles: To_IPO_14

Add

Routing Profiles
default

Routing Profile

Add

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport
					TLS

Routing Profile

URI Group	*	Time of Day	default
Load Balancing	Priority	NAPTR	□
Transport	None	Next Hop Priority	☑
Next Hop In-Dialog	□	Ignore Route Header	□
ENUM	□	ENUM Suffix	

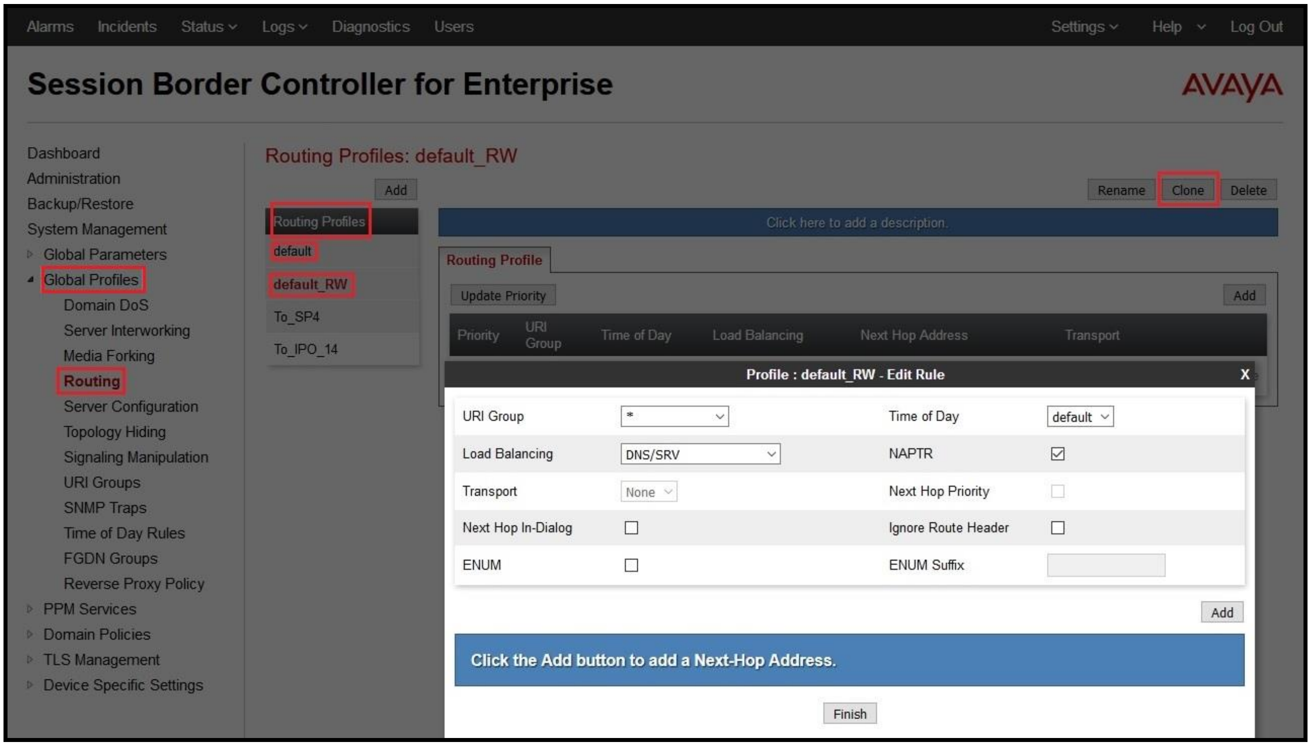
Add

Priority / Weight	Server Configuration	Next Hop Address	Transport	
1	IPO_14	10.10.98.14:5061 (TLS)	None	Delete

Back Finish

Figure 59 – Remote Worker Routing

From the menu on the left-hand side, select **Global Profiles → Routing**, select the existing **default Routing Profiles** and click on the **Clone** button, and name it **default_RW** and click **Finish** (not shown) to submit the changes. The **default_RW** was created as below.



URI Group	*	Time of Day	default
Load Balancing	DNS/SRV	NAPTR	☑
Transport	None	Next Hop Priority	□
Next Hop In-Dialog	□	Ignore Route Header	□
ENUM	□	ENUM Suffix	

Click the Add button to add a Next-Hop Address.

Figure 60 – Remote Worker Default Routing

The Routing Profile **To_IPO_14** is used in the Remote Worker Subscriber Flow (Refer to **Section 11.1.9.1**). The Routing Profile **default_RW** is used in the Remote Worker Server Flow (Refer to **Section 11.1.9.2**).

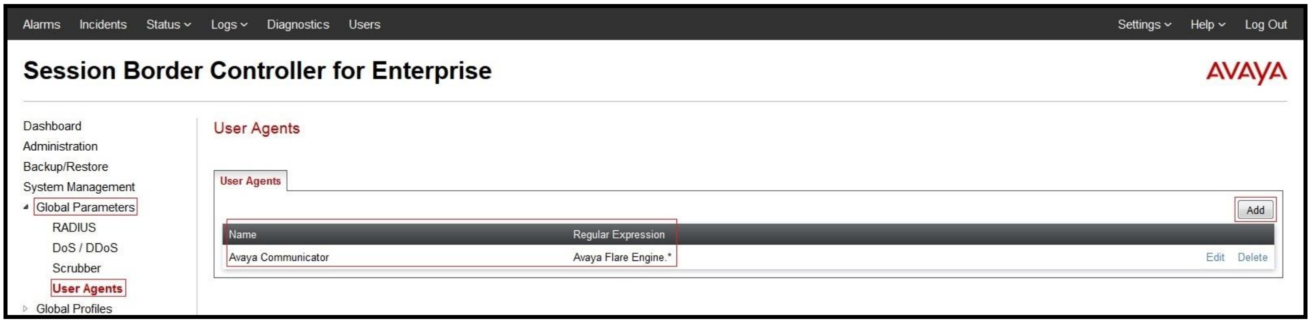
11.1.6. User Agent

User Agents are created for each type of Remote Worker endpoint used. In the compliance test, the Avaya Communicator for Windows (SIP) softphone was used, and its configuration is shown below. From the menu on the left-hand side, select **Global Parameters → User Agents**, and click **Add** button to create a new User Agent.

Enter the following:

- **Name** = **Avaya Communicator**
- **Regular Expression = Avaya Flare Engine.***

In this expression, "Avaya Flare Engine.*" will match any software version listed after the user agent name.



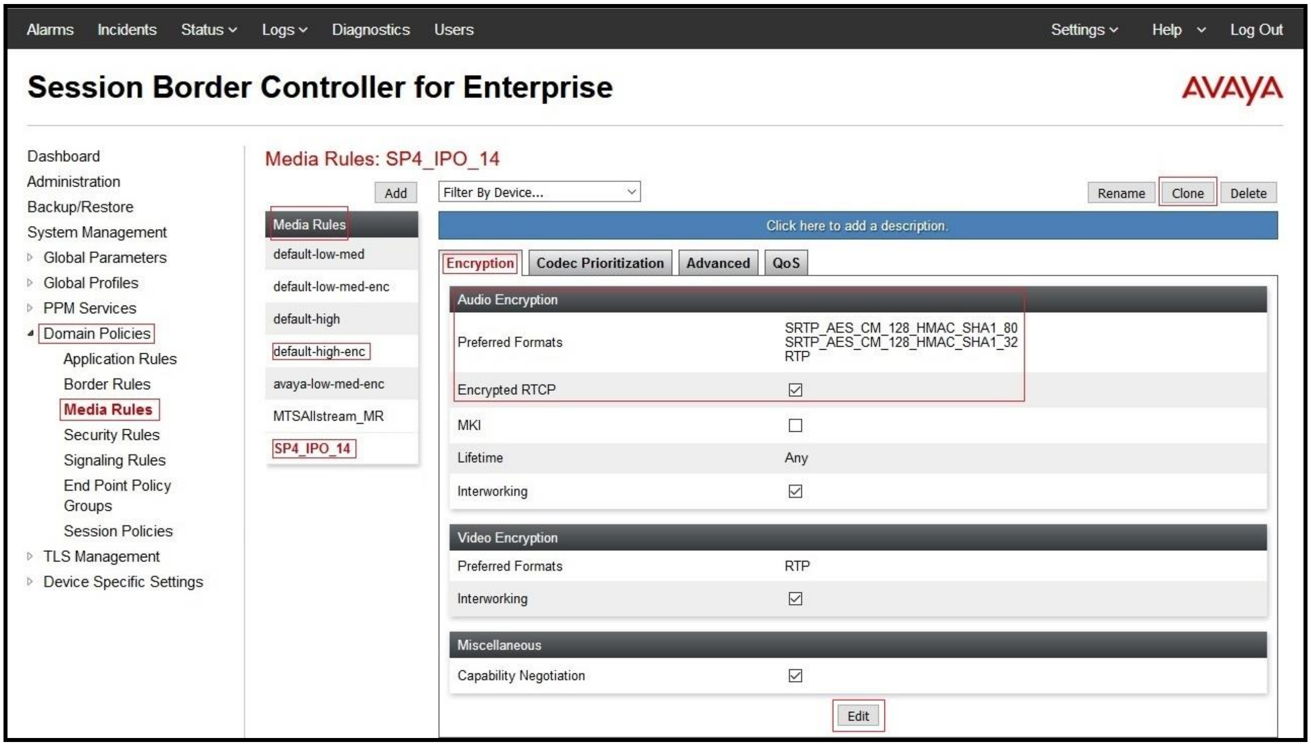
Name	Regular Expression
Avaya Communicator	Avaya Flare Engine.*

Figure 61 – Remote Worker User Agent

The **Avaya Communicator** User Agent is defined in the Remote Worker Subscriber Flow (see **Section 11.1.9.1**).

11.1.7. Create Media Rules for Remote Worker

Use the Media Rules SP4_IPO_14 defined in **Section 6.3.2** for remote worker



Media Rules: SP4_IPO_14

Audio Encryption	
Preferred Formats	SRTP_AES_CM_128_HMAC_SHA1_80 SRTP_AES_CM_128_HMAC_SHA1_32 RTP
Encrypted RTCP	☑
MKI	□
Lifetime	Any
Interworking	☑

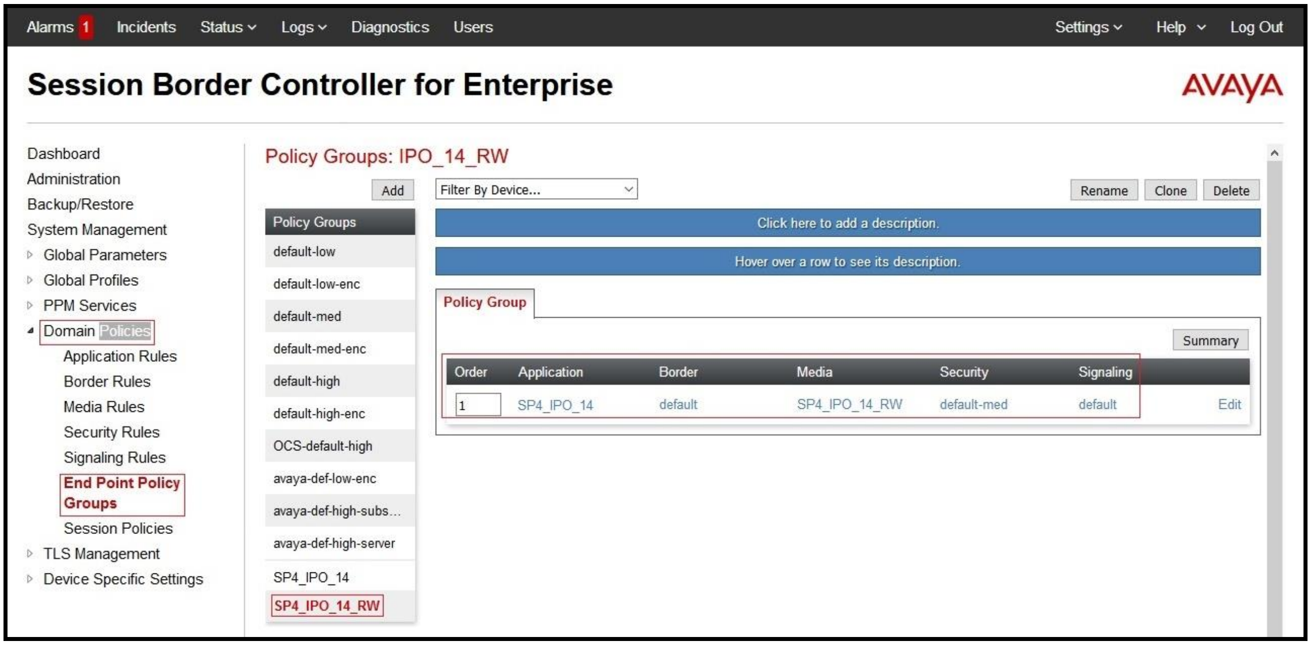
Video Encryption	
Preferred Formats	RTP
Interworking	☑

Miscellaneous	
Capability Negotiation	☑

Figure 62 – Remote Worker Media Rule

11.1.8. End Point Policy Groups

Use End Point Policy Group SP4_IPO_14 defined in **Section 6.3.3** for the Remote Worker connection.



Order	Application	Border	Media	Security	Signaling	
1	SP4_IPO_14	default	SP4_IPO_14_RW	default-med	default	Edit

Figure 63 – Remote Worker Endpoint Policy Group

End Point Policy Group **SP4_IPO_14** is used in the Subscriber Flow (Refer to **Section 11.1.9.1**) and in the Server Flow (Refer to **Section 11.1.9.2**).

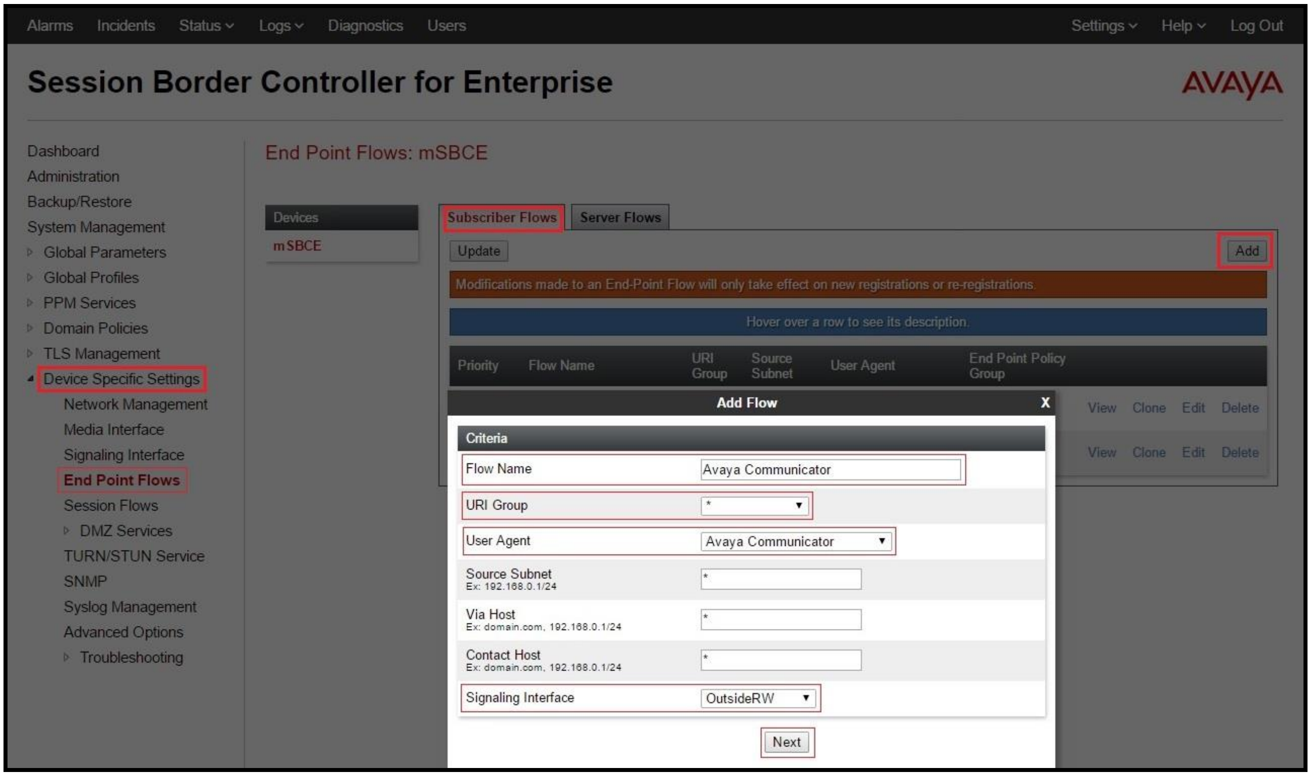
11.1.9. End Point Flows

A Subscriber Flow and a Server Flow are created for Remote Worker.

11.1.9.1 Subscriber Flow

A **Subscriber Flow** is defined as follows:
From the menu on the left-hand side, select **Device Specific Settings → End Point Flows**.
On **Subscriber Flows** tab, click on **Add** and the **Criteria** window will open.

- Enter **Flow Name** (e.g., **Avaya Communicator**).
- **URI Group** = *
- **User Agent** = **Avaya Communicator** (Refer to **Section 11.1.6**)
- **Source Subnet** = * (default)
- **Via Host** = * (default)
- **Contact Host** = * (default)
- **Signaling Interface** = **OutsideRW** (Refer to **Section 11.1.2**)



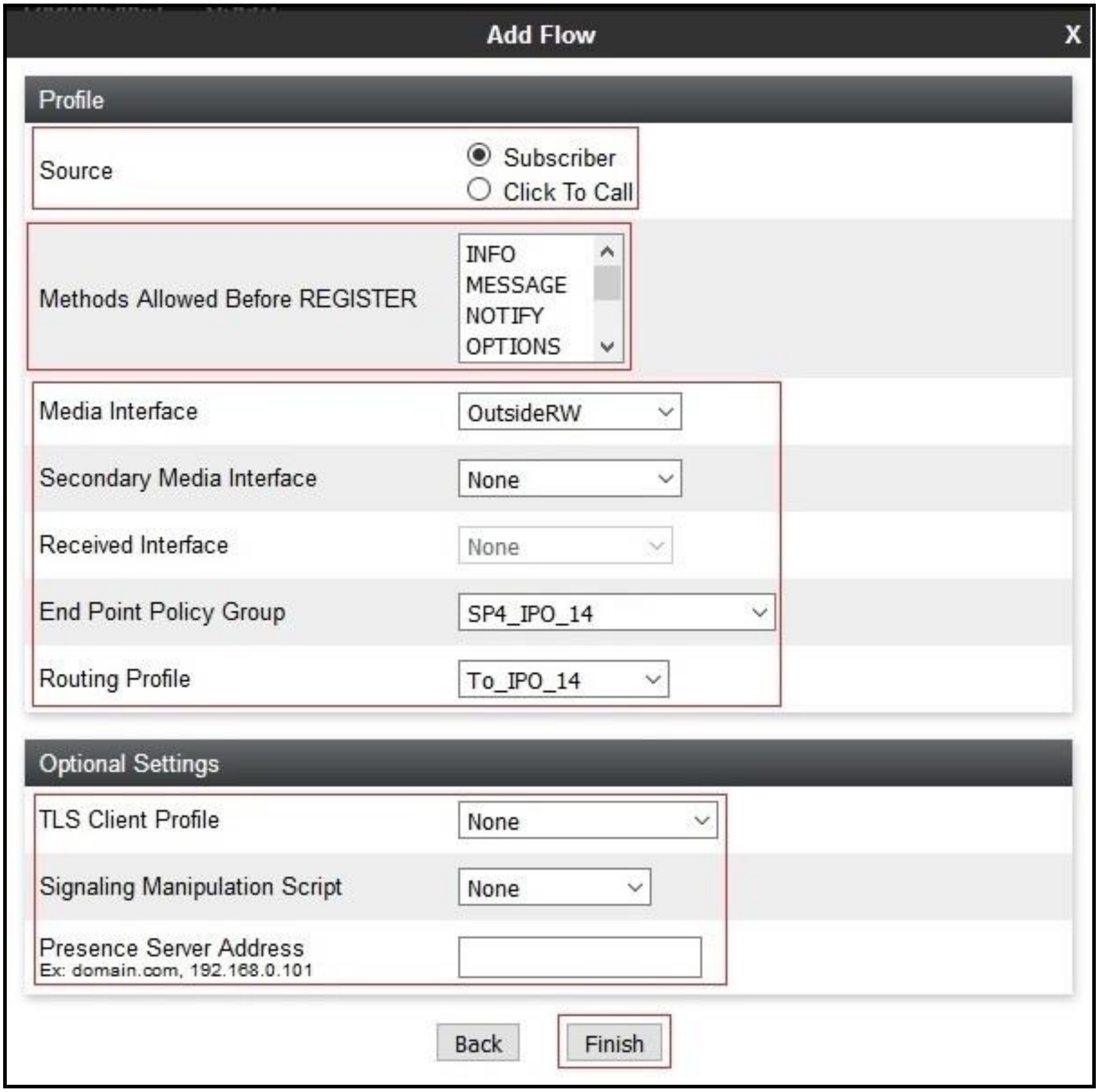
Criteria

Flow Name	Avaya Communicator
URI Group	*
User Agent	Avaya Communicator
Source Subnet Ex: 192.168.0.1/24	*
Via Host Ex: domain.com, 192.168.0.1/24	*
Contact Host Ex: domain.com, 192.168.0.1/24	*
Signaling Interface	OutsideRW

Figure 64 – Remote Worker Subscriber Flow 1

Click on **Next** and the **Profile** window will open. Enter the followings:

- **Source** = **Subscriber**
- **Methods Allowed Before REGISTER**: Leave as default.
- **Media Interface** = **OutsideRW** (Refer to **Section 11.1.3**)
- **Secondary Media Interface = None**
- **Received Interface = None**
- **End Point Policy Group = SP4_IPO_14** (Refer to **Section 11.1.8**)
- **Routing Profile = To_IPO_14** (Refer to **Section 11.1.5**)
- **TLS Client Profile** = **None**
- **Signaling Manipulation Script** = **None**
- **Presence Server Address** = **Blank**
- Click **Finish** to submit the changes.



Source: ● Subscriber ○ Click To Call

Methods Allowed Before REGISTER: INFO, MESSAGE, NOTIFY, OPTIONS

Media Interface: OutsideRW

Secondary Media Interface: None

Received Interface: None

End Point Policy Group: SP4_IPO_14

Routing Profile: To_IPO_14

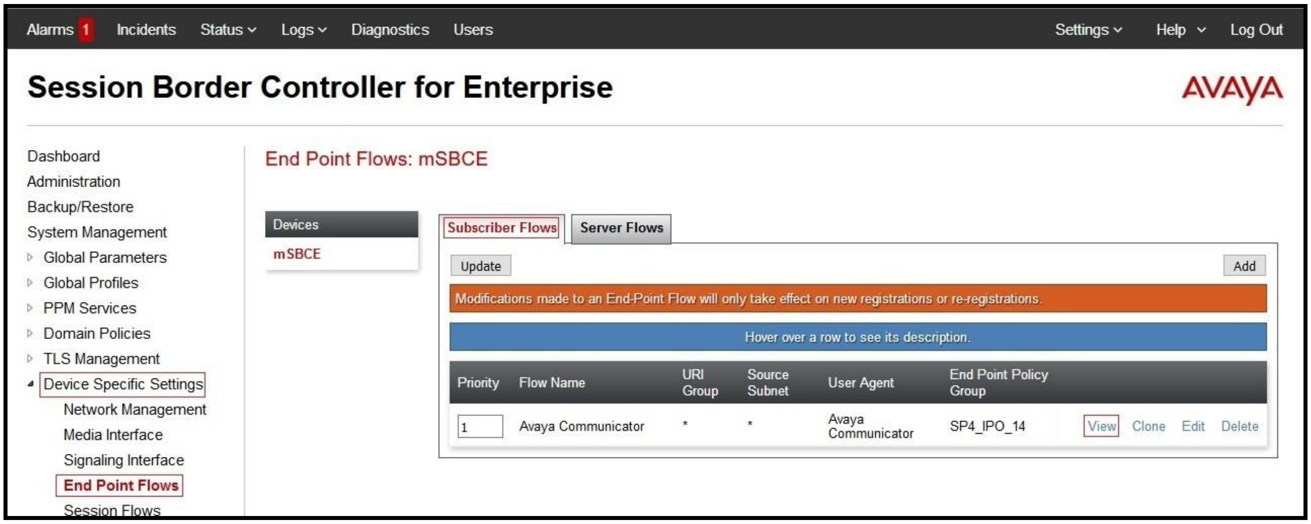
TLS Client Profile: None

Signaling Manipulation Script: None

Presence Server Address
Ex: domain.com, 192.168.0.101

Figure 65 – Remote Worker Subscriber Flow 2

The **Subscriber Flows** tab shown below displays the finished Subscriber Flow **Avaya Communicator**.



End Point Flows: mSBCE

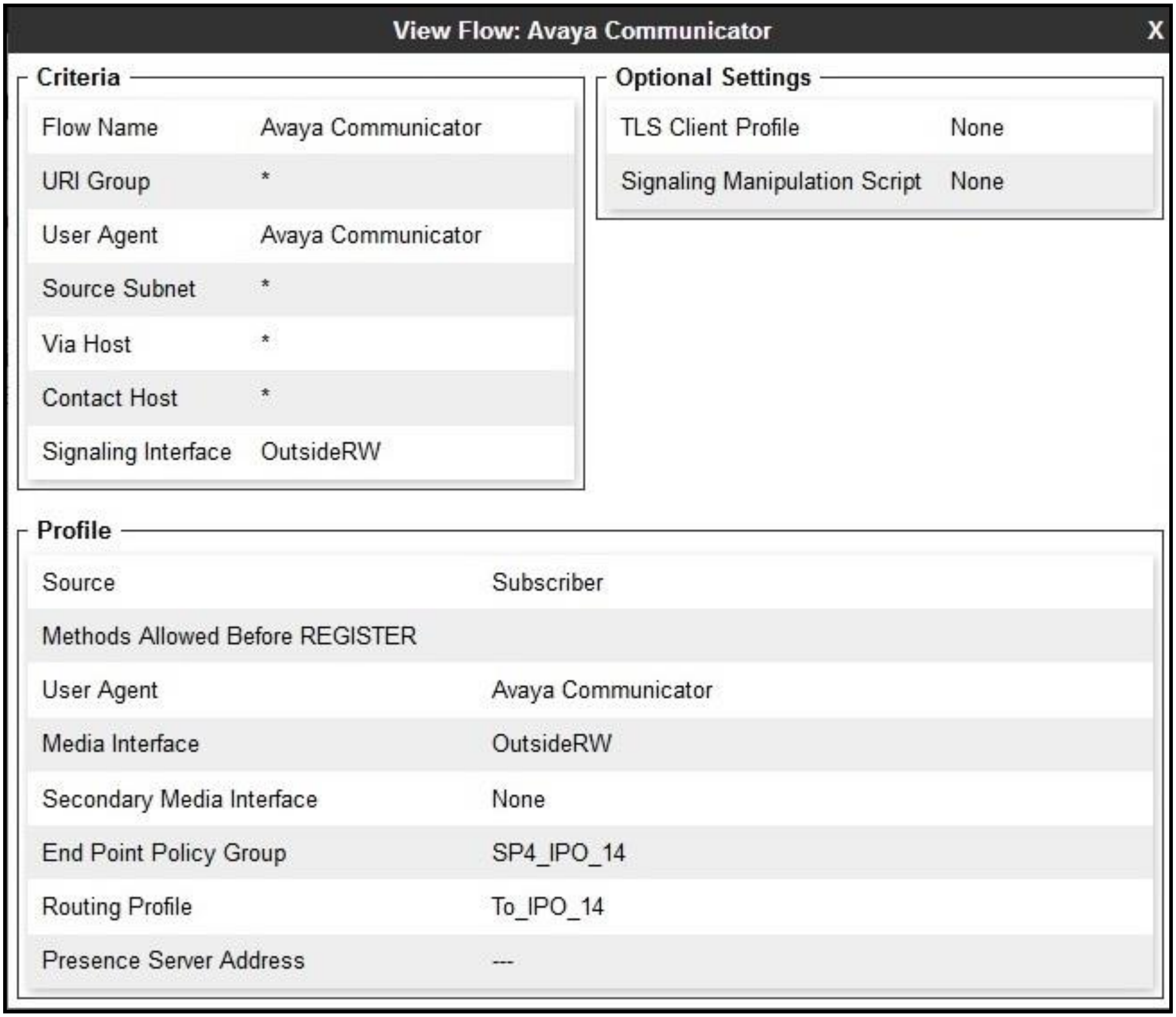
Modifications made to an End-Point Flow will only take effect on new registrations or re-registrations.

Hover over a row to see its description.

Priority	Flow Name	URI Group	Source Subnet	User Agent	End Point Policy Group
1	Avaya Communicator	*	*	Avaya Communicator	SP4_IPO_14

Figure 66 – Remote Worker Subscriber Flow 3

Click on the highlighted **View** link brings up the following **View Flow** window.



View Flow: Avaya Communicator

Criteria

Flow Name	Avaya Communicator
URI Group	*
User Agent	Avaya Communicator
Source Subnet	*
Via Host	*
Contact Host	*
Signaling Interface	OutsideRW

Optional Settings

TLS Client Profile	None
Signaling Manipulation Script	None

Profile

Source	Subscriber
Methods Allowed Before REGISTER	
User Agent	Avaya Communicator
Media Interface	OutsideRW
Secondary Media Interface	None
End Point Policy Group	SP4_IPO_14
Routing Profile	To_IPO_14
Presence Server Address	---

Figure 67 – Remote Worker Subscriber Flow 4

11.1.9.2 Server Flow

The following section shows the new **Server Flow** settings for Remote Worker. The new Remote Worker Server Flow (IPO_14_RW) is configured for the SIP traffic flow from Avaya IP Office to Remote Worker via Avaya SBCE.

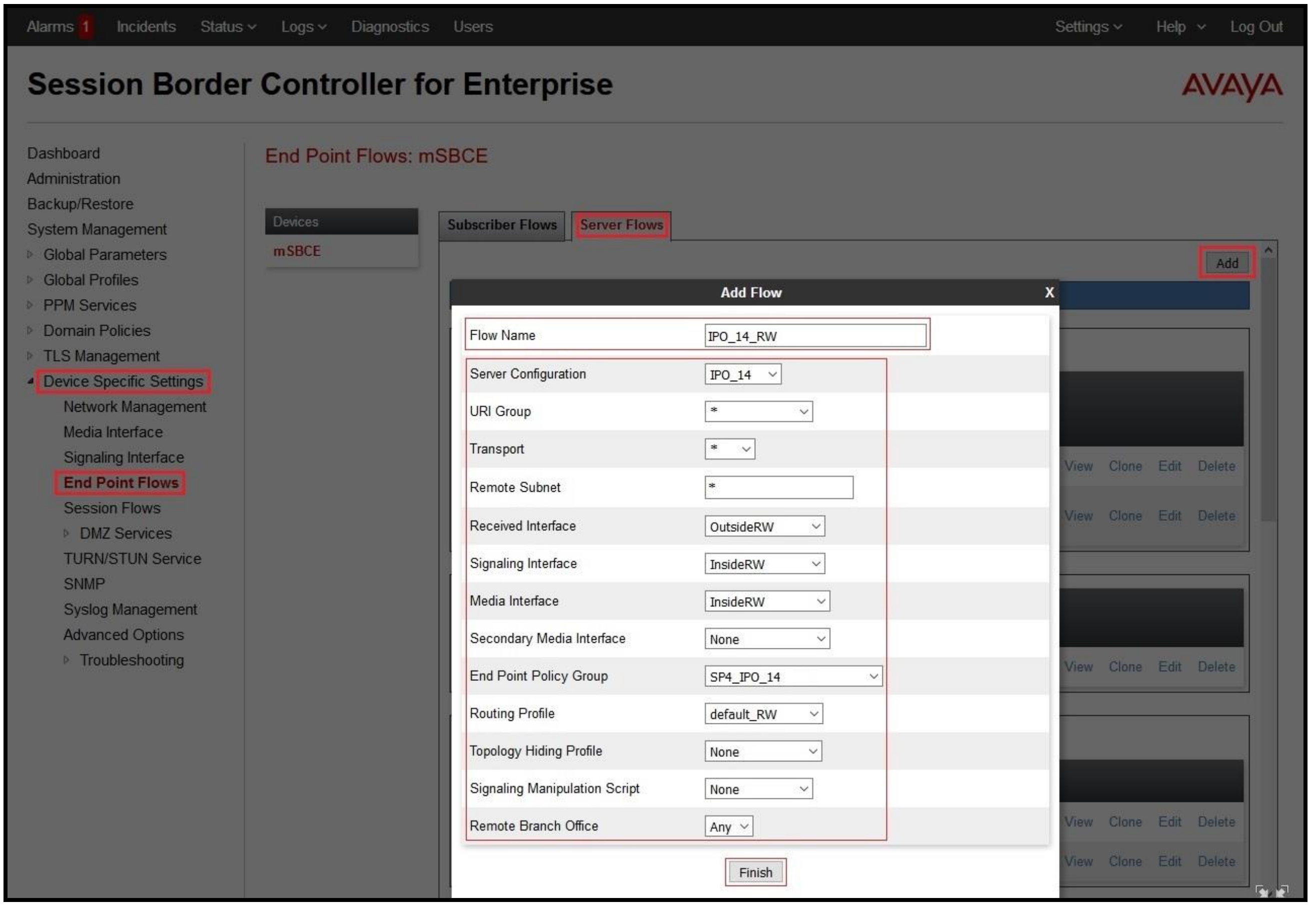
From the menu on the left-hand side, select **Device Specific Settings → End Point Flows**

On **Server Flows** tab, click on **Add** to create a new server flow for Remote Worker

Enter the following:

- **Flow Name = IPO_14_RW**
- **Server Configuration** = **IPO_14** (Refer to **Section 11.1.4**)

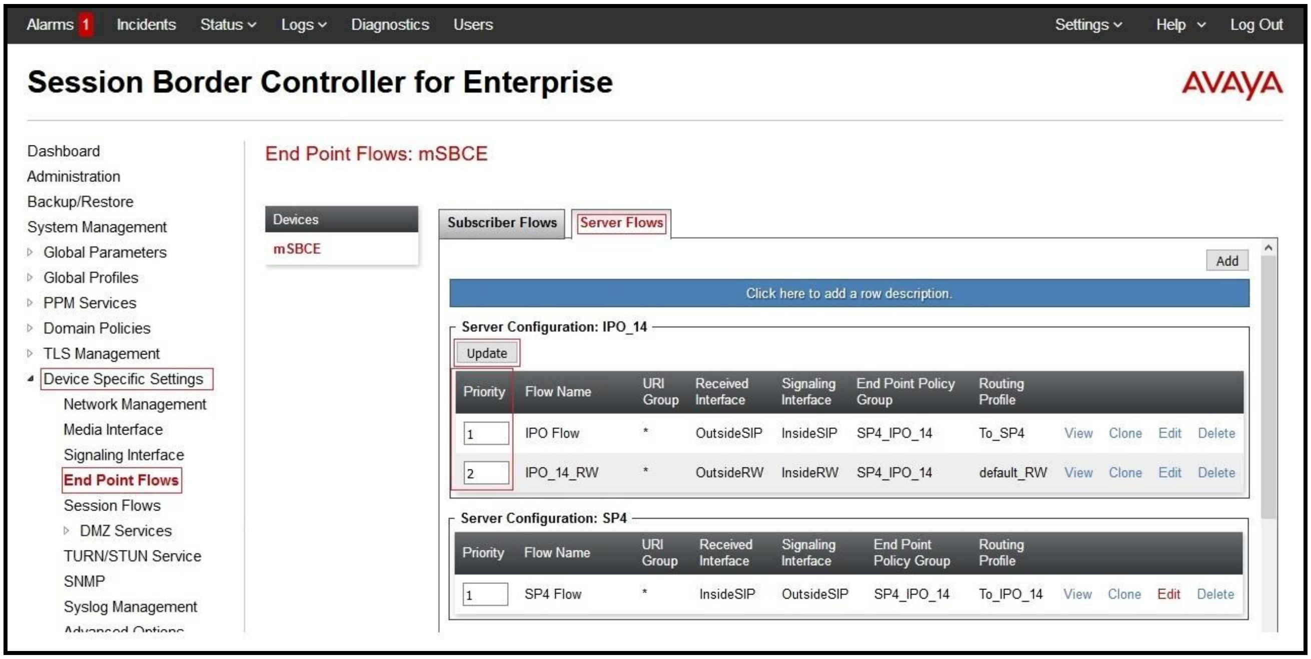
- **URI Group** = ***** (default)
- **Transport** = ***** (default)
- **Remote Subnet** = ***** (default)
- **Received Interface** = **OutsideRW** (Refer to **Section 11.1.2**)
- **Signaling Interface** = **InsideRW** (Refer to **Section 11.1.2**)
- **Media Interface** = **InsideRW** (Refer to **Section 11.1.3**)
- **Secondary Media Interface = None**
- **End Point Policy Group** = **SP4_IPO_14** (Refer to **Section 11.1.8**)
- **Routing Profile** = **default_RW** (Refer to **Section 11.1.5**)
- **Topology Hiding Profile** = **None**
- **Signaling Manipulation Script** = **None**
- **Remote Branch Office** = **Any**
- Click **Finish** to submit the changes



Flow Name	IPO_14_RW
Server Configuration	IPO_14
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	OutsideRW
Signaling Interface	InsideRW
Media Interface	InsideRW
Secondary Media Interface	None
End Point Policy Group	SP4_IPO_14
Routing Profile	default_RW
Topology Hiding Profile	None
Signaling Manipulation Script	None
Remote Branch Office	Any

Figure 68 – Remote Worker Server Flow 1

If the Remote Worker server flow is listed ahead of the flow for SIP Trunking **IPO Flow** (defined in **Section 6.4.4.1**), enter **2** in the **Priority** box at the start of the Remote Worker flow entry and click the **Update** button under the server name. The completed flow should show up in the **Server Flows** tab as below.



End Point Flows: mSBCE

Server Configuration: IPO_14

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	IPO Flow	*	OutsideSIP	InsideSIP	SP4_IPO_14	To_SP4	View	Clone	Edit	Delete
2	IPO_14_RW	*	OutsideRW	InsideRW	SP4_IPO_14	default_RW	View	Clone	Edit	Delete

Server Configuration: SP4

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	SP4 Flow	*	InsideSIP	OutsideSIP	SP4_IPO_14	To_IPO_14	View	Clone	Edit	Delete

Figure 69 – Remote Worker Server Flow 2

11.2. Remote Worker Endpoint Configuration on Avaya IP Office

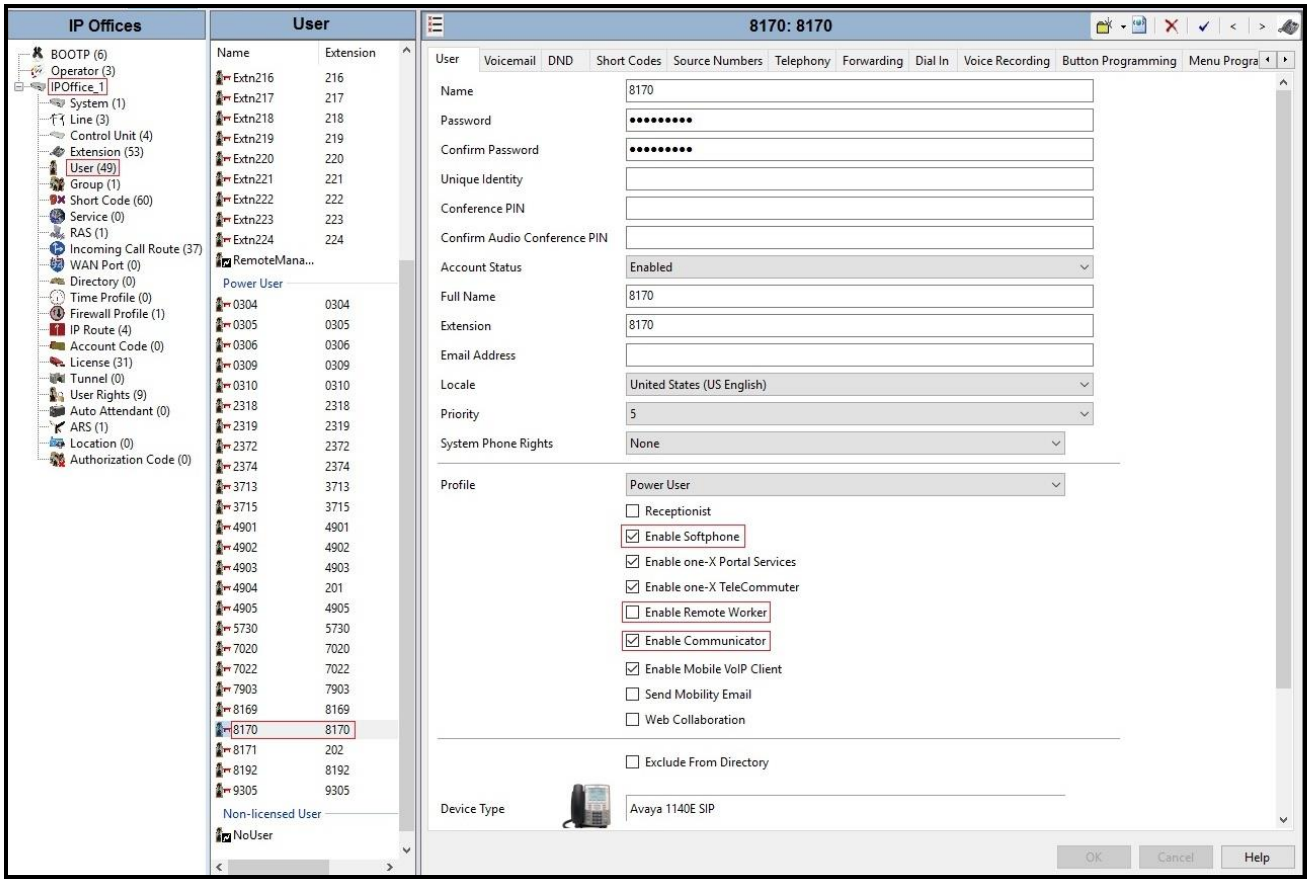
The Remote Worker - Avaya Communicator for Windows endpoint is added to the Avaya IP Office **User** and **Extension** configuration.

11.2.1. Extension and User Configuration

No special configurations are required to create the Remote Worker extension and user in Avaya IP Office. Follow the same standard procedures for creating a local extension and user for Avaya Communicator for Windows.

The Remote Worker user provisioned is shown below. Note that since the Remote Worker endpoint used in the reference configuration is Avaya Communicator for Windows, the **Enable Softphone** and **Enable Communicator** options are selected.

Note: Do not check the **Enable Remote Worker** option. This is only enabled for Avaya IP Office “native” Remote Worker configurations, not for Remote Worker configurations utilizing the Avaya SBCE.



Name	Extension
Extn216	216
Extn217	217
Extn218	218
Extn219	219
Extn220	220
Extn221	221
Extn222	222
Extn223	223
Extn224	224
RemoteMana...	
Power User	
0304	0304
0305	0305
0306	0306
0309	0309
0310	0310
2318	2318
2319	2319
2372	2372
2374	2374
3713	3713
3715	3715
4901	4901
4902	4902
4903	4903
4904	201
4905	4905
5730	5730
7020	7020
7022	7022
7903	7903
8169	8169
8170	8170
8171	202
8192	8192
9305	9305
Non-licensed User	
NoUser	

Name: 8170
Password: •••••••••
Confirm Password: •••••••••
Unique Identity:
Conference PIN:
Confirm Audio Conference PIN:
Account Status: Enabled
Full Name: 8170
Extension: 8170
Email Address:
Locale: United States (US English)
Priority: 5
System Phone Rights: None

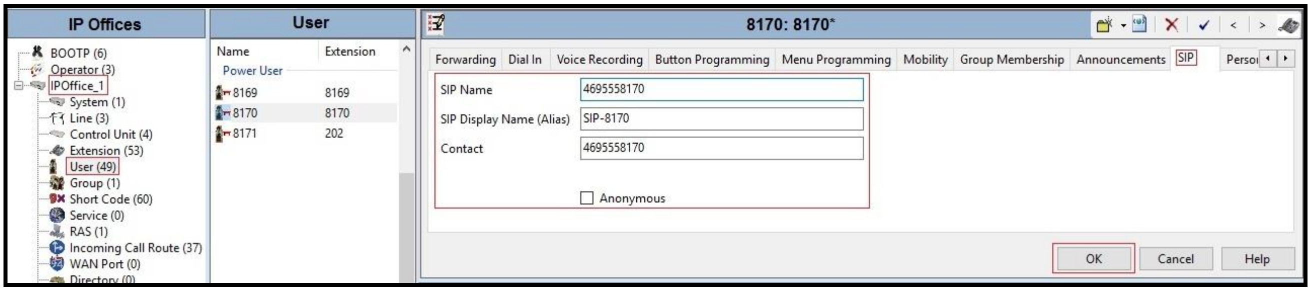
Profile: Power User
☐ Receptionist
☑ Enable Softphone
☑ Enable one-X Portal Services
☑ Enable one-X TeleCommuter
☐ Enable Remote Worker
☑ Enable Communicator
☑ Enable Mobile VoIP Client
☐ Send Mobility Email
☐ Web Collaboration

☐ Exclude From Directory

Device Type: Avaya 1140E SIP

Figure 70 – Remote Worker User Configuration 1

The **SIP** tab for the Remote User is configured the same way as with a local Avaya IP Office user (see **Section 5.8**).



SIP Name: 4695558170

SIP Display Name (Alias): SIP-8170

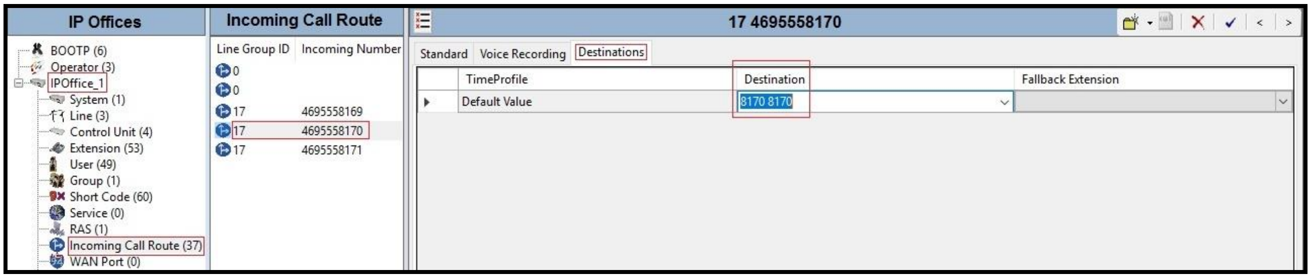
Contact: 4695558170

☐ Anonymous

Figure 71 – Remote Worker User Configuration 2

11.2.2. Incoming Call Route

Follow the same procedures described in **Section 5.9** for defining an Incoming Call Route to the Remote Worker.



Line Group ID	Incoming Number
0	
0	
17	4695558169
17	4695558170
17	4695558171

TimeProfile	Destination	Fallback Extension
Default Value	8170 8170	

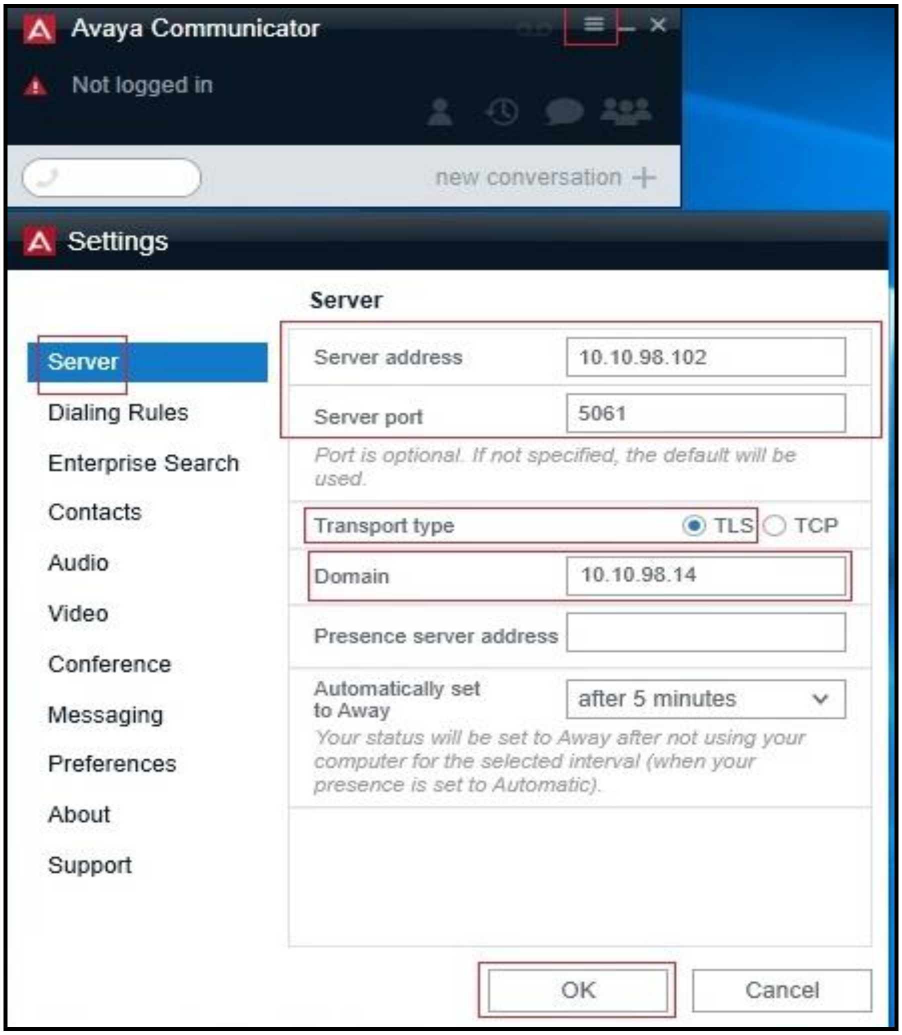
Figure 72 – Remote Worker Incoming Call Route

11.3. Remote Worker - Avaya Communicator for Windows Settings

The following screen illustrates Avaya Communicator for Windows administration settings for Remote Worker as used in the reference configuration.

After opening the Avaya Communicator for Windows application, select the **Settings** icon, select **Server** from the Settings menu, and enter the following:

- **Server address** = **10.10.98.102** (IP address of Remote Worker outside interface B1 on Avaya SBCE (see **Section 11.1.1**)
- **Server port** = **5061**
- **Transport type** = **TLS**
- **Domain** = **10.10.98.14** (SIP Domain Name was defined in LAN2→ VoIP tab in **Section 5.3**)
- Click **OK** the save the changes.



Server

Server address: 10.10.98.102

Server port: 5061

Port is optional. If not specified, the default will be used.

Transport type: ● TLS ○ TCP

Domain: 10.10.98.14

Presence server address:

Automatically set to Away: after 5 minutes

Your status will be set to Away after not using your computer for the selected interval (when your presence is set to Automatic).

Figure 73 – Remote Worker - Avaya Communicator for Windows Settings

Note: For this compliance testing, only audio calls were tested with RTP media for Avaya Communicator for Windows.

The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.